Google Inc. et al v. Egger et al
Doc. 441 Att. 9

Exhibit 10

Dockets.Justia.com

LEXSEE 72 GEO. WASH. L. REV. 1306

Copyright (c) 2004 The George Washington Law Review
The George Washington Law Review

August, 2004

72 Geo. Wash. L. Rev. 1306

LENGTH: 38229 words

THE FUTURE OF INTERNET SURVEILLANCE LAW: A SYMPOSIUM TO DISCUSS INTERNET SURVEILLANCE, PRIVACY & THE USA PATRIOT ACT: SURVEILLANCE LAW: RESHAPING THE FRAMEWORK: The System of Foreign Intelligence Surveillance Law

NAME: Peter P. Swire*

BIO: * Professor, Moritz College of Law of the Ohio State University and John Glenn Scholar in Public Policy Research. I thank the people with experience in foreign intelligence law who helped me in this project, many of whom prefer not to be identified. Stewart Baker, Jerry Berman, Jim Dempsey, John Podesta, and Ruth Wedgwood are among those who have helped teach me this topic. I am grateful for comments on earlier drafts from Susan Freiwald, Beryl Howell, Kim Lane Scheppele, Peter Raven-Hansen, Coleen Rowley, Stephen Saltzburg, Michael Vatis, and those who attended my presentations at the Association of American Law Schools annual conference, The George Washington University Law School, the Moritz College of Law, and the University of Toledo School of Law. My thanks to Najah Allen, Katy Delaney, Heather Hostetler, and Scott Zimmerman for research assistance, and to the Moritz College of Law and the John Glenn Institute for research support.

SUMMARY:
... The Foreign Intelligence Surveillance Act ("FISA") was enacted in 1978 to solve a long-simmering problem. ... The legal standard for "national security" or "foreign intelligence" surveillance results from the interaction of two conflicting positions. ... The statute required the Chief Justice to designate seven (now eleven) district court judges to the new Foreign Intelligence Surveillance Court ("FISC"). ... Although this Article has focused on the differences between Title III and foreign intelligence surveillance, a complete account of wiretap and electronic surveillance law requires the description of numerous other distinctions. ... In debates about U.S. wiretap law there is often an implicit assumption that Title III wiretaps are the "normal" means of surveillance, with FISA orders as an exception used for embassies and other foreign intelligence functions. ... The medical privacy rule specifically allows disclosure to the government for intelligence investigations and for reasons of national security, and the financial privacy laws allow delay of notice to the target of an investigation upon proper showings. ... Even if these individuals are considered "agents of a foreign power," it will be difficult to convince the FISC judges that this surveillance is "sufficiently important for foreign intelligence purposes" to justify a FISA order. ...

TEXT:
[*1307]

Introduction

The Foreign Intelligence Surveillance Act ("FISA") n1 was enacted in 1978 to solve a long-simmering problem. Since Franklin Roosevelt, presidents had asserted their "inherent authority" to authorize wiretaps and other surveillance for national security purposes. n2 Over time, the Supreme Court made clear that the Fourth Amendment required a neutral magistrate to issue a prior warrant for ordinary wiretaps used for domestic law enforcement purposes. n3 Yet the Supreme Court reserved a realm of "foreign intelligence" [*1308] wiretaps where the Court had not yet stated what procedures were required by the Fourth Amendment.

In the face of this uncertainty, both supporters and critics of surveillance had an incentive to compromise. Supporters of surveillance could gain by a statutory system that expressly authorized foreign intelligence wiretaps, lending the weight of congressional approval to surveillance that did not meet all the requirements of ordinary Fourth Amendment searches. Critics of surveillance could institutionalize a series of checks and balances on the previously unfettered discretion of the President and the Attorney General to conduct surveillance in the name of national security.

The basic structure of FISA remained unchanged from 1978 until the attacks of September 11, 2001. In the wake of those attacks, Congress quickly enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act"). n4 The Patriot Act made significant changes to FISA, notably by tearing down the "wall" that had largely separated foreign intelligence activities from the usual prosecution of domestic crimes. n5 The Patriot Act also greatly expanded the statutory authority to require libraries and other organizations to disclose records and tangible objects to federal investigators, while making it a criminal act to report that the disclosure had been made. n6 In related changes, Attorney General John Ashcroft loosened internal Justice Department Guidelines that had constrained investigators' discretion on how to investigate activities protected by the First Amendment. n7 Because the Patriot Act was passed so quickly, with only minimal hearings and debate in Congress, the FISA changes and other provisions of the Act are scheduled to sunset on December 31, 2005. n8

This period before the sunset will be the occasion for the most important debate on the system of foreign intelligence surveillance law since passage of the 1978 Act. In 2003, for the first time, the number of surveillance orders issued under FISA exceeded the number of law enforcement wiretaps issued nationwide. n9 This Article, drawing on both my academic and government experiences, n10 seeks to create a more informed basis for assessing how to [*1309] amend FISA and otherwise improve the ability of our foreign intelligence law to meet the twin goals of national security, on the one hand, and protection of the rule of law and civil liberties, on the other.

Part I of the Article discusses national security surveillance before 1978, tracing both the development of the Fourth Amendment for law enforcement wiretaps and the distinct legal authorities that recognized broader authority for the President in the areas of national security and foreign affairs. Part I also includes an examination of the history of abuses of national security surveillance in the period before 1978. These abuses, many of which were revealed in the course of the Watergate crisis, were a crucial education to Congress and the American people about the ways in which domestic security surveillance was often executed contrary to existing laws and in ways that posed serious threats to the democratic process.

Part II explains the 1978 compromises embodied in FISA and contrasts its special rules with the stricter rules that apply to wiretaps used in the ordinary criminal context. Part III examines the history of foreign intelligence surveillance law from 1978 until the attacks of September 11, 2001. Although the legal structure changed only incrementally during this time, the period was marked by a large increase in the number of FISA surveillance orders. This history suggests that FISA had met at least some of the goals of its drafters, regularizing and facilitating the surveillance power subject to institutional checks from all three branches of government. n11

Part IV charts the recent history of FISA. The expansion of FISA authority in the Patriot Act was limited for a time by the first publicly released decision of the Foreign Intelligence Surveillance Court, which was responding, in part, to more than seventy-five instances of misleading applications for FISA surveillance. n12 That decision, in turn, was reversed in the first-ever decision of the Foreign Intelligence Surveillance Court of Review, which essentially upheld the expanded Patriot Act powers against statutory and constitutional challenges. n13

Part V examines the system of foreign intelligence surveillance law. Because the usual Fourth Amendment and due process protections do not apply in individual cases, it becomes more important to have system-wide checks and balances against recurrence of the abuses of earlier periods. The Article explores the claim that "everything has changed" in the wake of September [*1310] 11. n14 That claim, if true, could justify expanded surveillance powers. There are significant counterarguments, however, that suggest the threats today are more similar than often recognized to the threats from earlier periods, undercutting the case for expanded powers.

Part VI then explores proposals for reform. Due to the classified nature of the foreign intelligence process, there are limits to the ability of outside commentators to assess details of the workings of the system of foreign intelligence surveillance law. Nonetheless, the changes since September 11 have been in the direction of eliminating a number of the important checks and balances that were created when Congress last had full discussions of foreign intelligence surveillance law. n15 The proposals for reform here can be considered as either concrete proposals or as a guide to the questions Congress should ask in its oversight of the system as the sunset approaches. In either event, more thorough vetting of institutional alternatives is necessary in wake of the very large changes to this area of law since the fall of 2001.

I. National Security Surveillance Before 1978

The legal standard for "national security" or "foreign intelligence" surveillance results from the interaction of two conflicting positions. The first position is that wiretaps taking place on American soil should be treated like wiretaps used for law enforcement purposes, with the same Fourth Amendment protections. The second position is that the President has special authority over national security issues, and therefore can authorize wiretaps with fewer or no Fourth Amendment limits. This Part of the Article examines the legal basis for the two positions and then examines the sobering history of problems arising from domestic surveillance before 1978.

A. The Fourth Amendment and Law Enforcement Wiretaps

The law for domestic wiretaps, used for law enforcement purposes, has evolved considerably in the past century. In the 1928 case Olmstead v. United States n16 the Supreme Court found no Fourth Amendment limits on a wiretap unless the wiretap was accompanied by physical trespass on a suspect's property. n17 Justice Brandeis famously dissented in Olmstead, saying that the Framers "conferred, as against the Government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men." n18 Congress responded to the decision by passing the Communications Act of 1934. n19 Although that statute provided federal standards for wiretaps, state officials could wiretap subject only to the often weak standards and enforcement of state laws. n20 Meanwhile, as discussed below, many federal [*1311] wiretaps were placed by agents who failed to comply with the Communications Act.

The law for domestic wiretaps changed decisively in the 1960s. In 1967, in Katz v. United States, n21 the Supreme Court held that full Fourth Amendment protections would apply to electronic surveillance of private telephone conversations. n22 Later Court decisions adopted the "reasonable expectation of privacy" test described in Justice Harlan's concurrence in Katz as the doctrinal test for when a probable cause warrant would be required under the Fourth Amendment. n23 The Supreme Court specifically reserved the issue of whether similar warrants were required for wiretaps done for national security purposes. n24

Also in 1967, the Supreme Court applied the Fourth Amendment to wiretaps performed by state officials in Berger v. New York. n25 In doing so, the Supreme Court gave detailed guidance to legislatures about what sort of protections were appropriate for wiretaps for law enforcement purposes. n26 For purposes of this Article, it is important to note two required safeguards that have not necessarily applied to national security wiretaps: (1) judicial supervision of wiretaps; and (2) notice to the subject of the wiretap after the wiretap has expired. n27

Congress responded the next year in Title III of that year's crime bill. n28 The basic rules for these "Title III" wiretaps were quite strict, with multiple requirements that do not apply to the usual probable cause warrant for a physical search. The Title III rules generally apply today to law enforcement wiretaps in the United States, as discussed further below.

[*1312] The Electronic Communications Privacy Act of 1986 ("ECPA") n29 was the next significant legal change to the regime for domestic electronic surveillance. Whereas Title III applied to "wire" and "oral" communications, i.e., to phone wiretaps and bugs, ECPA extended many of the same protections to e-mail and other "electronic" communications. n30 The Title III and ECPA rules then remained largely unchanged until the Patriot Act in 2001, when the privacy protections for domestic wiretaps were loosened in a number of respects. n31 Notwithstanding these recent changes, the essential structure of Title III and ECPA remains in effect today, including the requirement of judicial supervision of wiretaps, the need to give notice to the object of surveillance once the wiretap is completed, and the obligation to minimize the amount of surveillance in order to prevent intrusions that are outside of the law enforcement investigation.

B. The Law and Logic of National Security Wiretaps

This history of applying the Fourth Amendment and the rule of law to wiretaps is accompanied by a second history, that of using wiretaps and other surveillance tools to protect the national security. Consider the Cold War example of an employee of the Soviet Embassy. What should the standards have been for wiretaps of that employee, who might also be an agent of the KGB? A Title III wiretap would often be impossible to get, because there would be no probable cause that a crime had been or would be committed. Yet this potential or known spy plausibly posed a serious threat to national [*1313] security. A wiretap might create extremely useful intelligence about the Soviet agent's confederates and actions.

For many people, including those generally inclined to support civil liberties, the example of a known spy operating within the United States provides an especially compelling case for allowing wiretaps and other surveillance. Spies operating within the United States pose a direct threat to national security. For instance, spies can and have turned over nuclear and other vital military secrets to foreign powers. n32 At the same time, some of the usual safeguards on wiretaps seem inappropriate when applied to foreign agents. Notifying the target of a criminal wiretap after the fact is required by the notice component of the Fourth Amendment and can be a crucial safeguard because it alerts citizens and the press of any overuse or abuse of the wiretap power. By contrast, notifying a foreign agent about a national security power can compromise sources and methods and create a diplomatic scandal. Similarly, minimization in the domestic context helps preserve the privacy of individuals who are not the target of a criminal investigation. Minimization in the foreign intelligence context, by contrast, can mean discarding the only hints available about the nature of a shadowy and hard-to-detect threat to security.

During wartime especially, it is easy to see how the temptation to use "national security" wiretaps against spies and foreign enemies, even on U.S. soil, would be irresistible. The legal basis for such a national security power can be derived from the text of the Constitution. The President is named Commander in Chief of the armed forces, and domestic actions against foreign powers may be linked to military and intelligence efforts abroad. This explicit grant of power to the President is supplemented by vague and potentially very broad language in Article II of the Constitution, that the President shall exercise the "executive power" and "take Care that the Laws be faithfully executed." n33 Going beyond the text, the Supreme Court in 1936, in United States v. Curtiss-Wright Export Corp., n34 relied on the structure of the Constitution and the nature of sovereign nations to establish the "plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations." n35

President Franklin Roosevelt, responding to the Second World War, was the first President to authorize wiretaps on national security grounds. n36 The use of such wiretaps expanded during the Cold War. In 1967, in Katz, the Supreme Court declined to extend its holding to cases "involving the national [*1314] security." n37 In 1971, Justice Stewart summarized the expansion of the executive power that "in the two related fields of national defense and international relations[,] ... largely unchecked by the Legislative and Judicial branches, has been pressed to the very hilt since the advent of the nuclear missile age." n38

The Supreme Court finally addressed the lawfulness of national security wiretaps in 1972 in United States v. United States District Court, n39 generally known as the "Keith" case after the name of the district court judge in the case. n40 The defendant, Plamondon, was charged with the dynamite bombing of an office of the Central Intelligence Agency in Michigan. n41 During pretrial proceedings, the defendants moved to compel the United States to disclose electronic surveillance information that had been obtained without a warrant. n42 The Attorney General submitted an affidavit stating that he had expressly approved the wiretaps, which were used "to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." n43 The United States objected to disclosure of the surveillance materials, claiming that the surveillance was a reasonable exercise of the President's power (exercised through the Attorney General) to protect the national security. n44 Both the district court and the circuit court held for the defendant.n45

The Supreme Court unanimously affirmed. n46 Justice Powell's opinion found that Title III, by its terms, did not apply to the protection of "national security information" and that the statute did not limit "'the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means.'" n47 As it turned to the constitutional discussion of the scope of the Fourth Amendment, the Court expressly reserved the issues of foreign intelligence surveillance that are now covered by FISA: "The instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." n48

The Court then turned to the question left open by Katz: "'Whether safeguards other than prior authorization by a magistrate would satisfy the [*1315] Fourth Amendment in a situation involving the national security.'" n49 The Government sought an exception to the Fourth Amendment warrant requirement, relying on the inherent presidential power and duty to "'preserve, protect, and defend the Constitution of the United States.'" n50 The Court acknowledged the importance of that duty, yet held that a warrant issued by a neutral magistrate was required for domestic security wiretaps. n51 Noting the First Amendment implications of excessive surveillance, the Court concluded: "Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent." n52

While recognizing the potential for abuse in domestic security wiretaps, the Court also recognized the "different policy and practical considerations from the surveillance of 'ordinary crime.'" n53 The list of possible differences is entirely familiar to those engaged in the debates since September 11: the gathering of security intelligence is often for a long term; it involves "the interrelation of various sources and types of information"; the "exact targets of such surveillance may be more difficult to identify"; and there is an emphasis on "the prevention of unlawful activity." n54 In light of these differences, the nature of "reasonableness" under the Fourth Amendment can shift somewhat. The Court invited legislation: "Congress may wish to consider protective standards for ... [domestic security] which differ from those already prescribed for specified crimes in Title III." n55 The Court specifically suggested creating a different standard for probable cause and designating a special court to hear the wiretap applications, n56 two invitations taken up by Congress in FISA.

C. National Security Wiretaps and "The Lawless State"

The Supreme Court's invitation was eventually accepted by Congress in 1978 in FISA. n57 FISA was enacted at a unique time, in the wake of Watergate and spectacular revelations about illegal actions by U.S. intelligence agencies. In my opinion, anyone who wishes to debate FISA and possible amendments to it has a responsibility to consider the history of this period. I am not a pessimist who believes that intelligence activities inevitably will return to the level of lawlessness at that time. I do believe, however, that human nature has remained largely unchanged since then. Unless effective institutional safeguards exist, large and sustained expansions of domestic intelligence [*1316] activity, in the name of national security, can quite possibly recreate the troublesome behaviors of the past.

One particularly detailed account of the earlier period is a 1977 book by Morton Halperin, Jerry Berman and others entitled The Lawless State: The Crimes of the U.S. Intelligence Agencies. n58 That book devotes an annotated chapter to the illegal surveillance activities of several U.S. agencies - the FBI, the CIA, the Army, the IRS, and others. The most famous discussion of the deeds and misdeeds of the intelligence agencies are the reports by the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, known as the "Church Committee" after its chairman, Frank Church. n59 The 1976 final report summarized the number of people affected by domestic intelligence activity:

FBI headquarters alone has developed over 500,000 domestic intelligence files, and these have been augmented by additional files at FBI Field Offices. The FBI opened 65,000 of these domestic intelligence files in 1972 alone. In fact, substantially more individuals and groups are subject to intelligence scrutiny than the number of files would appear to indicate, since typically, each domestic intelligence file contains information on more than one individual or group, and this information is readily retrievable through the FBI General Name Index.

The number of Americans and domestic groups caught in the domestic intelligence net is further illustrated by the following statistics:

- Nearly a quarter of a million first class letters were opened and photographed in the United States by the CIA between 1953-1973, producing a CIA computerized index of nearly one and one-half million names.

- At least 130,000 first class letters were opened and photographed by the FBI between 1940-1966 in eight U.S. cities.

- Some 300,000 individuals were indexed in a CIA computer system and separate files were created on approximately 7,200 Americans and over 100 domestic groups during the course of CIA's Operation CHAOS (1967-1973).

- Millions of private telegrams sent from, to, or through the United States were obtained by the National Security Agency from 1947 to 1975 under a secret arrangement with three United States telegraph companies.

- An estimated 100,000 Americans were the subjects of United States Army intelligence files created between the mid 1960s and 1971.

[*1317] - Intelligence files on more than 11,000 individuals and groups were created by the Internal Revenue Service between 1969 and 1973 and tax investigations were started on the basis of political rather than tax criteria.

- At least 26,000 individuals were at one point catalogued on an FBI list of persons to be rounded up in the event of a "national emergency." n60

These statistics give a flavor for the scale of domestic surveillance. Rather than repeat the history in detail here, it is helpful to identify themes that show the important concerns raised by improper surveillance. These are discussed below.

1. Routine Violations of Law

In The Lawless State the authors identify and document literally hundreds of separate instances of criminal violations by intelligence agencies. n61 The Church Committee reported "frequent testimony that the law, and the Constitution were simply ignored." n62 The Committee quoted testimony from the man who headed the FBI's Intelligence Division for ten years: "Never once did I hear anybody, including myself, raise the question: 'Is this course of action which we have agreed upon lawful, is it legal, is it ethical or moral.' We never gave any thought to this line of reasoning, because we were just naturally pragmatic." n63 Instead of concern for the law, the intelligence focus was on managing the "flap Potential" - the likely problems if their activities became known. n64

2. Expansion of Surveillance for Prevention and Other Purposes

After World War II, "preventive intelligence about 'potential' espionage or sabotage involved investigations based on political affiliations and group membership and association. The relationship to law enforcement was often remote and speculative ... ." n65 Until the Church Committee's hearings, the FBI continued to collect domestic intelligence under "sweeping authorizations" for investigations of "'subversives,' potential civil disturbances, and 'potential crimes.'" n66 Based on its study of the history, the Church Committee concluded:

> The tendency of intelligence activities to expand beyond their initial scope is a theme which runs through every aspect of our investigative findings. Intelligence collection programs naturally generate [*1318] ever-increasing demands for new data. And once intelligence has been collected, there are strong pressures to use it against the target. n67

3. Secrecy

An essential aspect of domestic intelligence was secrecy:

> Intelligence activity ... is generally covert. It is concealed from its victims and is seldom described in statutes or explicit executive orders. The victim may never suspect that his misfortunes are the intended result of activities undertaken by his government, and accordingly may have no opportunity to challenge the actions taken against him. n68

It was only in the wake of the extraordinary events of Watergate and the resignation of President Richard Nixon that Congress and the public had any inkling of the scope of domestic intelligence activities. That realization of the scope led directly to thoroughgoing legal reforms (many of which are being rolled back or questioned in the wake of September 11).

4. Use Against Political Opponents

The Church Committee documented that: "Each administration from Franklin D. Roosevelt's to Richard Nixon's permitted, and sometimes encouraged, government agencies to handle essentially political intelligence." n69 Wiretaps and other surveillance methods were used on members of Congress, Supreme Court Justices, and numerous mainstream and nonmainstream political figures. The level of political surveillance and intervention grew over time. n70 By 1972, tax investigations at the IRS were targeted at protesters against the Vietnam War, n71 and "the political left and a large part of the Democratic party [were] under surveillance." n72

5. Targeting and Disruption of Unpopular Groups, Including the Civil Rights Movement

The FBI's COINTELPRO - counterintelligence program - "was designed to 'disrupt' groups and 'neutralize' individuals deemed to be threats to national security." n73 Targets for infiltration included the Ku Klux Klan and the Black Panthers. A special target was Martin Luther King, Jr., from late 1963 until his death in 1968. The Church Committee report explained:

[*1319]

In the words of the man in charge of the FBI's "war" against Dr. King, "No holds were barred... . The program to destroy Dr. King as the leader of the civil rights movement included efforts to discredit him with executive branch officials, Congressional leaders, foreign heads of state, American ambassadors, churches, universities, and the press." n74

In one especially ugly episode, Dr. King was preparing to go to Sweden to receive the Nobel Peace Prize when the FBI sent him an anonymous letter threatening to release an embarrassing tape recording unless he committed suicide. n75

6. Chilling of First Amendment Rights

The FBI's COINTELPRO program targeted "speakers, teachers, writers, and publications themselves." n76 One internal FBI memorandum "called for 'more interviews' with New Left subjects 'to enhance the paranoia endemic in these circles' and 'get the point across there is an FBI agent behind every mailbox.'" n77 Once a federal agency is trying to get the message out that there is an "agent behind every mailbox," then the chilling effect on First Amendment speech can be very great indeed.

7. Harm to Individuals

The hearings in the 1970s produced documented cases of harm to individuals from intelligence actions. For instance, an anonymous letter to an activist's husband accused his wife of infidelity and contributed strongly to the breakup of the marriage. n78 Also, "a draft counsellor deliberately, and falsely, accused of being an FBI informant was 'ostracized' by his friends and associates." n79 In addition to "numerous examples of the impact of intelligence operations," the Church Committee concluded that "the most basic harm was to the values of privacy and freedom which our Constitution seeks to protect and which intelligence activity infringed on a broad scale." n80

8. Distortion of Data to Influence Government Policy and Public Perceptions

Used properly, intelligence information can provide the President and other decisionmakers with the most accurate information possible about risks to national security. The Church Committee found that intelligence agencies sometimes warped intelligence to meet their political goals:

[*1320]

The FBI significantly impaired the democratic decisionmaking process by its distorted intelligence reporting on communist infiltration of and influence on domestic political activity. In private remarks to Presidents and in public statements, the Bureau seriously exaggerated the extent of communist influence in both the civil rights and anti-Vietnam war movements. n81

9. Cost and Ineffectiveness

The Church Committee concluded: "Domestic intelligence is expensive... Apart from the excesses described above, the usefulness of many domestic intelligence activities in serving the legitimate goal of protecting society has been questionable." n82 After reviewing the effectiveness of various aspects of domestic intelligence, the Committee's chief recommendation was "to limit the FBI to investigating conduct rather than ideas or associations." n83 The Committee also specifically recommended continued "intelligence investigations of hostile foreign intelligence activity." n84

In summary, the history shows numerous concrete examples of lawbreaking by the U.S. intelligence agencies. More generally, the history helps show how secret information gathering and disruption of political opponents over time can threaten democracy itself. The fear is that leaders using "dirty tricks" and secret surveillance can short-circuit the democratic process and entrench themselves in power. The legal question is how to construct checks and balances that facilitate needed acts by the government but which also create long-term checks against abuse.

II. The 1978 Compromise: The Foreign Intelligence Surveillance Act

At the level of legal doctrine, FISA was born from the two legal traditions discussed in Part I: the evolving Supreme Court jurisprudence that wiretaps required judicial supervision, and the continuing national security imperative that at least some foreign intelligence wiretaps be authorized. At the level of practical politics, FISA arose from the debate between the intelligence agencies, who sought maximum flexibility to protect national security, and the civil libertarians, who argued that the abuses revealed by the Church Committee should be controlled by new laws and institutions. n85

The clear focus of FISA, as shown by its title, was on foreign rather than domestic intelligence. The statute authorized wiretaps and other electronic surveillance against "foreign powers." n86 These "foreign powers" certainly included the communist states arrayed against the United States in the Cold War. The definition was broader, however, including any "foreign government [*1321] or any component thereof, whether or not recognized by the United States." n87 A "foreign power" included a "faction of a foreign nation," or a "foreign-based political organization, not substantially composed of United States persons." n88 Even in 1978, the definition also included "a group engaged in international terrorism or activities in preparation therefor." n89

Surveillance could be done against an "agent of a foreign power," which classically would include the KGB agent or someone else working for a foreign intelligence service. n90 An "agent of a foreign power" could also include a person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power." n91 The definition of "international terrorism" had three elements: violent actions in violation of criminal laws; an intent to influence a government by intimidation or coercion; and actions that transcend national boundaries in their method or aims. n92

The Act drew distinctions between U.S. persons and non-U.S. persons. n93 The former consists essentially of U.S. citizens and permanent residents. n94 Non-U.S. persons could qualify as an "agent of a foreign power" simply by being an officer or employee of a foreign power, or a member of an international terrorist group. n95 The standards for surveillance against U.S. persons were stricter, in line with the Church Committee concerns about excessive surveillance against domestic persons. U.S. persons qualified as an "agent of a foreign power" only if they knowingly engaged in listed activities, such as clandestine intelligence activities for a foreign power, which "involve or may involve a violation of the criminal statutes of the United States." n96

In FISA, Congress accepted in large measure the invitation in Keith to create a new judicial mechanism for overseeing national security surveillance. n97 The new statute used the terms "foreign power" and "agent of a foreign power" employed by the Supreme Court in Keith, where the Court specifically said that its holding applied to domestic security wiretaps rather [*1322] than surveillance of "foreign powers." n98 Instead of creating a special regime for domestic security, however, Congress decided to split surveillance into only two parts - the procedures of Title III, which would apply to ordinary crimes and domestic security wiretaps, and the special procedures of FISA, which would apply only to "agents of a foreign power." n99

A curious hybrid emerged in FISA between the polar positions of full Title III protections, favored by civil libertarians, and unfettered discretion of the executive to authorize national security surveillance, favored by the intelligence agencies. The statute required the Chief Justice to designate seven (now eleven) district court judges to the new Foreign Intelligence Surveillance Court ("FISC"). n100 These judges had jurisdiction to issue orders approving electronic surveillance upon finding a number of factors, notably that "there is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power." n101 This probable cause standard looks to quite different facts than the Title III standard, which requires "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense" for wiretaps to be permitted. n102

FISA orders contain some, but not all, of the other safeguards in Title III. Both regimes require high-level approval within the Department of Justice, with the Attorney General having to give personal approval for FISA applications. n103 Both regimes require minimization procedures to reduce the effects on persons other than the targets of surveillance. n104 Both provide for electronic surveillance for a limited time, with the opportunity to extend the surveillance. n105 Both require details concerning the targets of the surveillance and the nature and location of the facilities placed under surveillance. n106 Both allow "emergency" orders, where the surveillance can begin without judicial approval subject to quick, subsequent approval by a judge. n107

[*1323] As for differences, Title III gives discretion to the judge to refuse to issue the order, even where the statutory requirements have been met. n108 Under FISA, however, the judge "shall" issue the order once the statutory find-

ings are met. n109 FISA has looser standards about whether other, less-intrusive surveillance techniques must first be exhausted. n110

The most important difference is that the existence of a Title III wiretap is disclosed to the subject of surveillance after the fact, in line with the Fourth Amendment requirement that there be notice of government searches. n111 By sharp contrast, the FISA process is cloaked in secrecy. Targets of FISA surveillance almost never learn that they have been subject to a wiretap or other observation. The only statutory exception is where evidence from FISA surveillance is used against an individual in a trial or other proceeding. In such instances, the criminal defendant or other person can move to suppress the evidence on the grounds that the information was unlawfully acquired or the surveillance did not comply with the applicable order. Even in this setting the individuals have no right to see the evidence against them. The judge, upon a motion by the Attorney General, reviews the evidence in camera (in the judge's chambers) and ex parte (without assistance of defense counsel). n112

The secrecy and ex parte nature of FISA applications are a natural outgrowth of the statute's purpose, to conduct effective intelligence operations against agents of foreign powers. n113 In the shadowy world of espionage and counter-espionage, nations that are friends in some respects may be acting contrary to U.S. interests in other respects. Prudent foreign policy may suggest keeping tabs on foreign agents who are in the United States, but detailed disclosure of the nature of that surveillance could create embarrassing incidents or jeopardize international alliances.

Along with the limited nature of judicial supervision, Congress decided to create additional institutional checks on the issuance of the secret FISA [*1324] wiretaps. To regularize congressional oversight, the Attorney General must report to the House and Senate Intelligence Committees every six months about FISA electronic surveillance, including a description of each criminal case in which FISA information has been used for law enforcement purposes. n114 The Attorney General also must make an annual report to Congress and the public about the total number of applications made for orders and extensions of orders, as well as the total number that were granted, modified, or denied. n115 This report is similar to that required for Title III wiretaps, but the latter provides additional details such as the types of crimes for which a wiretap is used and the number of wiretaps that resulted in successful prosecutions. n116 Although the FISC ruled against an order for the first time in 2002, as described below, n117 the annual FISA reports provide a rough guide of the extent of FISA surveillance. n118

Congress also relied on institutional structures within the executive branch to check overuse of domestic surveillance. n119 The requirement that the Attorney General authorize applications meant that the FBI on its own could no longer implement national security wiretaps. Applications by the FBI would need to be approved by the Justice Department. In light of the historical evidence about the independence of longtime FBI Director J. Edgar Hoover from control by the Justice Department, n120 and the disagreements that have often continued between the FBI and the Department, n121 this supervision by the Justice Department was a potentially significant innovation in FISA.

Reacting to the historical evidence about surveillance of political speech and association, the 1978 statute provided that "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States." n122 This language reflects a congressional concern about infringement on First Amendment activities, but provides only modest safeguards, [*1325] because an individual could apparently be considered an agent of a foreign power based "largely" or "substantially" on protected activities.

Finally, the text of the 1978 statute showed that the purpose of the FISA wiretaps was foreign intelligence rather than preventing or prosecuting crimes. The Church Committee and other revelations of the 1970s had shown that the FBI had used the risk of "subversion" and other potential crimes as the justification for investigating a vast array of political and other domestic activity. n123 The 1978 statute therefore specified that the application for a FISA order certify that "the purpose of the surveillance is to obtain foreign intelligence information." n124

In summary, the 1978 FISA revealed a grand compromise between the advocates for civil liberties and the intelligence community. From the civil liberties side, FISA had the advantage of creating a legal structure for foreign intelligence surveillance that involved Article III judges. It had the disadvantage of having standards that were less protective overall than were constitutionally and statutorily required for investigations of domestic crimes. In particular, the notice requirement of the Fourth Amendment did not apply, and targets of FISA surveillance usually never learned they were the objects of government searches. From the intelligence perspective, FISA had the disadvantage of imposing bureaucratic rules and procedures on searches that had previously been done subject to the inherent authority of the President or the Attorney General. An advantage, which became more evident over time, was that FISA provided legislative legitimation for secret wiretaps, and created standardized bureaucratic procedures for getting them. By establishing these clear procedures, it became easier over time for the number of FISA surveillance orders to grow. To describe the compromise in another way, FISA set limits on surveillance by "The Lawless State," but gave "The Lawful State" clear rules that permitted surveillance.

III. FISA from 1978 to 2001

FISA was part of a broad-based effort in the wake of Watergate to place limits on the Imperial Presidency and its surveillance activities. n125 The Privacy Act of 1974 clamped down on secret files on Americans and created new legal rules for how personal information could be used by federal agencies. n126 The Freedom of Information Act was broadened substantially in 1974, n127 and greater openness in government was encouraged by the Government [*1326] in the Sunshine Act, n128 new rules in legislatures to open up committee hearings to the public, n129 and more aggressive investigative journalism in the wake of the revelations by Bob Woodward and Carl Bernstein. n130

The FBI in particular had to change its operations, including its domestic surveillance activities, in the wake of the revelations about "The Lawless State." The best-known limits on the FBI's activities were the Guidelines on Domestic Surveillance issued by Attorney General Edward Levi in 1976 ("Levi Guidelines"). n131 The guidelines limited domestic security investigations to activities that both "involve or will involve the use of force or violence" and "involve or will involve the violation of federal law." n132 The Levi Guidelines defined procedures and time limits for preliminary, limited, and full investigations. The FBI was required to report in detail about investigations to the Department of Justice, and the Attorney General or his designees had the power to terminate investigations at any time. To address concerns about intrusion into First Amendment activity, the Guidelines stated that all domestic security investigations "shall be designed and conducted so as not to limit the full exercise of rights protected by the Constitution and laws of the United States." n133

The Levi Guidelines represented a judgment that the best way to save the FBI as an effective agency was to demonstrate that it had come within the rule of law. Greater oversight of investigations by the Justice Department was central to the new approach: "If the FBI would play by the new rules, the Justice Department would defend it to the hilt." n134 The FBI likely shifted over time to a much higher compliance with legal rules than had been true before the revelations of the 1970s. n135

[*1327] The implementation of FISA after 1978 followed a similar pattern of Justice Department oversight of the FBI. Mary Lawton, the lead drafter of the Levi Guidelines, eventually became the chief of the Office of Intelligence Policy and Review ("OIPR") within the Justice Department. n136 Previously, the FBI had forum shopped in different parts of the Justice Department to get approval for domestic surveillance. Now the OIPR became the gatekeeper for all applications to the FISC. Mary Lawton, who had finished first in her class at the Georgetown Law Center, sat at the center of the process, applying "Mary's Law" to applications for FISA surveillance. n137

The 1996 book Main Justice, which provides the most detailed public writing about the period, summarizes the combined effect of having FISA applications signed by the intelligence agent, the lawyer who drafted it, the head of the intelligence agency, and the Attorney General:

All those signatures served a purpose, to assure the federal judge sitting in the FISA court that a national security wiretap was being sought for "intelligence purposes" and for no other reason - not to discredit political enemies of the White House, not to obtain evidence for a criminal case through the back door of a FISA counterintelligence inquiry. n138

This is consistent with my view of perhaps the most controversial change in FISA in the Patriot Act - the breaking down of the "wall" between foreign intelligence and law enforcement activities. My own understanding is that the wall has existed since the creation of FISA in 1978, but there has always been a gate in it. The OIPR has been the gatekeeper. It has permitted foreign intelligence information to go to law enforcement in a limited number of cases, but it has historically remained mindful of the basic dictate of FISA, that the purpose of FISA surveillance was for foreign intelligence and that there should be safeguards on the domestic surveillance that had created such problems in the period of "The Lawless State."

This understanding is consistent with the text of FISA and the actions of the Justice Department in 1995. As discussed above, the text of the original FISA stated that "the purpose" of the surveillance was "to obtain foreign intelligence information." n139 The text also provided mechanisms for using information from FISA wiretaps in court, subject to special rules about in camera review by the judge of the FISA material. n140 Taken together, the text [*1328] suggests a preponderance of use of the special wiretaps for foreign intelligence, with use for law enforcement only where the evidence was developed in the course of a bona fide foreign intelligence surveillance. n141 In 1995, two years after the death of Mary Lawton, Attorney General Janet Reno issued confidential guidelines to formalize procedures for contacts among the FBI, the Criminal Division, and OIPR for foreign intelligence and foreign counterintelligence investigations. n142 The guidelines gave OIPR a central role in the process. Both the FBI and the Criminal Division, for instance, were required to notify OIPR of contacts with each other concerning such investigations, and contacts between the FBI and the Criminal Division were logged. n143 The FBI was generally prohibited from contacting any U.S. Attorney's Office concerning such investigations without prior permission of both OIPR and the Criminal Division. n144 OIPR was further directed to inform the FISC "of the existence of, and basis for, any contacts among the FBI, the Criminal Division, and a U.S. Attorney's Office, in order to keep the FISC informed of the criminal justice aspects of the ongoing investigation." n145

Alongside these developments in the Justice Department, FISA changed only modestly from 1978 until the events of September 11, 2001. Federal courts upheld FISA against constitutional challenges. n146 The courts also upheld some broadening of the purpose requirement, allowing surveillance where "the primary purpose," rather than "the purpose," was to gather foreign intelligence information. n147

Although FISA originally applied only to electronic surveillance, Congress gradually widened its scope to other tools commonly used by law enforcement in criminal cases. After Attorney General Reno relied on her inherent powers to authorize physical surveillance of CIA spy Aldrich Ames's home, the Justice Department requested and received the authority in 1995 to apply to the FISC for physical searches. n148 In 1998, the Act was extended to include pen register and trap and trace orders (listing of the telephone [*1329] numbers and similar information contacted by an individual). n149 The same year, the Act was extended to permit access to limited forms of business records, notably including vehicle rental records of the sort relevant to investigations of the Oklahoma City and first World Trade Center bombings. n150 These extensions were analogous to FISA electronic surveillance, with the primary purpose to gather information on foreign powers or agents of foreign powers.

The most significant change was likely the increased number of FISA orders. Once the FISA system was up and running in 1981, there remained between 433 and 600 orders for each year through 1994, except for a one-year total of 635 in 1984. n151 In 1995, 697 orders were granted, growing in subsequent years to 839, 748, 796, 880, and 1012 during President Clinton's term. n152 FISA orders fell to 934 in 2001, and grew to record numbers of 1228 in 2002 and 1727 in 2003. n153 By comparison, the number of federal Title III wiretap orders in 1981 was 106, with a peak of 601 in 1999 and a total of 578 in 2003, the most recent year for which statistics are available. n154 State law enforcement also conducted Title III wiretaps, with a total of 861 reported for 2002. n155 Taken together, FISA wiretaps have grown substantially in the past decade, especially after September 11. Since the early 1980s they have constituted the majority of federal wiretaps.

In assessing the implementation of FISA from 1978 to early 2001, the basic structures from the 1970s remained fairly fixed. The bargain of FISA had been realized - the government could carry out secret surveillance in the United States, subject to limits to "foreign intelligence" activities and oversight by all three branches of government. The "wall" was in place, with the OIPR as the chief gatekeeper for exchange of information between the foreign intelligence and law enforcement operations. Despite the Levi Guidelines, there were some instances where civil liberties proponents produced evidence that "domestic surveillance" had interfered with First Amendment activities, but these instances seemed fairly few. n156 There was some expansion of legal authority, but the greatest practical change was likely the increased number of FISA applications over time, especially since efforts to fight terrorism climbed during the 1990s. n157

[*1330]

IV. The Patriot Act, the New Guidelines, and New Court Decisions

The attacks of September 11 led to the greatest changes by far in FISA law and practice since its creation in 1978. This Part examines the statutory amendments in the Patriot Act, new Attorney General guidelines on foreign intelligence surveillance and domestic security investigations, and the first published decisions by the FISC and the Foreign Intelligence Surveillance Court of Review ("FISCR").

A. The Patriot Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act") n158 was proposed by the Bush administration one week after the attacks of September 11 and signed into law on October 26, 2001. n159 Among the numerous changes in the law, the focus here is on three topics: the permission for FISA orders to have only "a significant purpose" of foreign intelligence; the use of FISA orders to get any "tangible object"; and the expansion of national security letters.

1. From "Primary Purpose" to "A Significant Purpose"

The 1978 law required the application for a FISA order to certify that "the purpose of the surveillance is to obtain foreign intelligence information." n160 As discussed above, a number of circuit courts interpreted this language to mean that the "primary purpose" of the order must be to obtain foreign intelligence information. n161 To ensure that the purpose of criminal law enforcement did not predominate, the "wall" was created between law enforcement and foreign intelligence investigations.

The Bush administration proposed that the text should change so that "a purpose" would be for foreign intelligence information. n162 After debate in Congress, the Patriot Act finally provided that "a significant purpose" must exist in order to obtain foreign intelligence information. n163 A separate provision emphasized that Congress wished to promote information sharing between criminal investigations and foreign intelligence investigations. n164 The [*1331] implications of these legislative changes were the subject of first published opinions by the FISC and the FISCR, and are discussed further below.

2. FISA Orders for any "Tangible Object"

Section 215 of the Patriot Act expanded the sweep of FISA orders to compel production of business records and other tangible objects. n165 The original FISA had focused on electronic surveillance and had not created a FISA mechanism for the government to get business records. After the Oklahoma City and first World Trade Center bombings, Congress authorized the use of FISA orders for travel records only. n166

Section 215 contained two statutory changes that drastically expanded this power. First, the type of records subject to the order went far beyond travel records. Now the search can extend to "any tangible things (including books, records, papers, documents, and other items)." n167 By its terms, the statute apparently would allow a FISA order to trump other laws that usually govern the release of records, including for medical records and other categories of records, that are generally subject to privacy protections.

Second, the legal standard changed for obtaining the order. Previously, the application had to show "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." n168 This standard, although less than probable cause, is relatively strict. The Patriot Act eliminated the need for any particularized showing. The application need merely "specify that the records concerned are sought for an authorized investigation ... to protect against international terrorism or clandestine intelligence activities." n169 What counts as an authorized investigation is within the discretion of the executive branch.

Under this change in the text, FISA orders can now apply to anyone, not only the target of the investigation. Previously, the records or other objects sought had to concern either a foreign power or the agent of a foreign power. Now, the FISA order can require production of records about persons who [*1332] have nothing to do with a foreign power. n170 The only weak restraints include the need for "an authorized investigation" and the requirement that surveillance of U.S. persons not be based solely upon First Amendment activities. n171 This is a significant change, permitting seizure of records of persons who are not the target of an investigation and not an agent of a foreign power. n172 Similarly, by permitting the order to cover records of all persons, the literal terms of section 215 would permit an entire database to be the subject of a FISA order. As long as there is "an authorized investigation," the statute does not set any limits on the type or number of records subject to the FISA order. n173

It is true that the range of records available to the government in criminal investigations has also expanded in recent decades. n174 One important safeguard in the criminal area, however, is that the records must be sought in connection with a crime that has been, is, or will be committed. In addition, as discussed further below, n175 section 215 contains what is often called a "gag rule" - "No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section." n176 No similar rule applies to business records produced in the course of a criminal investigation.

3. Expansion of "National Security Letters"

The Patriot Act significantly expanded the scope of the little-known tool of "National Security Letters" ("NSLs"). These are essentially the foreign intelligence corollary to administrative subpoenas for criminal investigations. Before the Patriot Act, NSLs allowed for access to certain records listed by statute, such as subscriber information for phone companies and Internet Service Providers and basic account information from banks and credit reporting agencies. n177

[*1333] The amendments to NSLs track the changes in section 215. Previously, there was the same significant showing required for each record, that "there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power." n178 The Patriot Act requires only that the records be "relevant" to an authorized investigation, and no longer requires that the target of the request be a foreign power or agent of a foreign power. n179

The Patriot Act broadened the sorts of investigations that qualify for NSLs for telephone and transactional records. Before, NSLs applied only to an "authorized foreign counter-intelligence operation." n180 Now they apply to "an authorized investigation to protect against international terrorism or clandestine intelligence activities." n181 The Patriot Act also lowered the level of official who could authorize an NSL. Previously, clearance had to come from a position of at least "Deputy Assistant Director." n182 Now, a "Special Agent in Charge" in a bureau field office may authorize an NSL, without any clearance by FBI headquarters. n183

The expanded scope of NSLs likely deserves significant attention because they operate without the participation of a judge and individuals never receive notice that the records have been sought. n184 Federal officials have stated that NSLs have become more common and been used at least "scores" of times since September 11. n185 Moreover, the Bush administration has sought approval for the CIA and the Pentagon to use NSLs inside of the United States, without the participation of the FBI or the Department of Justice. n186

4. Other Changes in the Patriot Act

There were other FISA amendments in the Patriot Act that will not be the subject of detailed analysis here. For example, the standard for getting a FISA pen register or trap and trace order was simplified in the Patriot Act. Previously, these orders could only be issued if there was reason to believe that the telephone line subject to the order had been or was about to be used in communications involving international terrorism or an agent of a foreign power. n187 That requirement was dropped in the Patriot Act, with the standard [*1334] becoming essentially the same as for domestic orders. The order can issue where the information is "relevant to an ongoing investigation." n188

The Patriot Act also extended "roving" wiretaps to FISA. Wiretap orders historically were linked to an individual telephone. With changing technology, individuals more often used multiple phones and other communications facilities. Congress approved the use of law enforcement wiretaps linked to an individual - roving wiretaps - in 1986. n189 The Patriot Act permitted roving wiretaps under FISA for the first time, "in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person." n190

The pen register and roving wiretap provisions, like the "significant purpose" test and section 215, sunset on December 31, 2005, although existing investigations can proceed under the Patriot Act even if there is no extension of the statutory authority. n191

B. New Guidelines in the Department of Justice

There have been numerous changes in the FBI and the Department of Justice since September 11 as the organizations have sought to respond to the terrorist threat. One overall pattern has been to discard earlier Department of Justice policies that set limits on foreign and domestic intelligence gathering. Proponents have seen these changes as overdue efforts to eliminate red tape. Critics have feared that important safeguards are being eliminated

The "wall" between foreign intelligence and law enforcement has come under particular challenge. Some changes began immediately after September 11. Previously, Justice Department guidelines had required the expert office of Justice, the OIPR, to be present at all meetings and discussions between the FBI and the Criminal Division for many FISA cases. After the attacks, OIPR no longer participated in all such meetings and instead reviewed a daily briefing book to inform itself and the FISC about those discussions. n192

The procedures for information sharing were greatly streamlined in "Intelligence Sharing Procedures" approved by Attorney General Ashcroft on [*1335] March 6, 2002 ("Ashcroft Guidelines"). n193 These new guidelines were designed "to permit the complete exchange of information and advice between intelligence and law enforcement officials." n194 They eliminated the prior restriction on prosecutors or other law enforcement officials "directing or controlling" the use of FISA surveillance. n195 They allowed the exchange of advice between the FBI, OIPR, and the Criminal Division regarding "the initiation, operation, continuation, or expansion of FISA searches or surveillance." n196 In short, the new guidelines sought to remove entirely the wall that limited information sharing between foreign intelligence and criminal investigations.

In May 2002, Attorney General Ashcroft rolled back another set of limitations on surveillance that had been put in place during the 1970s. The Levi Guidelines had set strict limitations on domestic security investigations, including rules designed to ensure that First Amendment activities were not improperly the subject of surveillance. n197 The new guidelines comprehensively revised the Levi Guidelines. Attorney General Ashcroft said that "terrorism prevention is the key objective under the revised guidelines." n198 He stressed that "unnecessary procedural red tape must not interfere with the effective detection, investigation, and prevention of terrorist activities." n199 An analysis by Jerry Berman and Jim Dempsey of the Center for Democracy and Technology highlighted three civil liberties concerns with the changes. n200 First, the guidelines gave new authority to FBI agents to attend public meetings and events of domestic groups without the need for suspicion of criminal or terrorist activity. Second, the guidelines authorized routine mining of commercial databases for personal information about citizens and organizations with no limitations on sharing and retention of that data. Finally, the guidelines reduced internal FBI supervision of the various stages of investigation, especially by expanding the use of preliminary inquiries where there is no reasonable indication of criminal or terrorist conduct.

[*1336]

C. Decisions by the FISA Courts

Passage of the Patriot Act and changes in the guidelines concerning the "wall" led to the first published decisions of the FISC and the FISCR. n201

The FISC decision was issued in May 2002 and became public as a result of oversight led by then-Chairman Patrick Leahy of the Senate Judiciary Committee. n202 The opinion, agreed to by all seven judges of the FISC, ordered detailed procedures to maintain the "wall" between foreign intelligence and criminal investigations. n203 The statutory basis for the decision was the requirement in FISA that there be minimization procedures. n204 The statute requires the Attorney General to create procedures "that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." n205 The court found that the March 2002 guidelines for information sharing were not reasonably designed to meet the statutory requirement. n206

One factor in the court's decision appears to have been its frustration about "an alarming number of instances" where the existing 1995 guidelines limiting information sharing had been violated. n207 In a series of reports to the court beginning in March 2000 the government admitted to misstatements and omissions of material facts in over seventy-five FISA applications. n208 "In virtually every instance," the FISC wrote, "the government's misstatements and omissions ... involved information sharing and unauthorized disseminations to criminal investigators and prosecutors." n209

The FISC also clearly believed that the "wall" was an established and integral part of the overall structure of FISA. n210 The court relied on the text of FISA that referred to the need to "obtain, produce, and disseminate foreign intelligence information." n211 In the view of the FISC, the primary purpose of FISA surveillance must be foreign intelligence information. That [*1337] information could later be used in criminal prosecutions only if it was initially collected with a foreign intelligence purpose in mind.

That interpretation of the statute was rejected on appeal. The three judges in the FISCR, federal appellate judges named by Chief Justice Rehnquist, issued an opinion that was distinctly friendly to information sharing and hostile to any continuation of the "wall." n212 The court found that the distinction between surveillance for foreign intelligence and surveillance for law enforcement was a "false dichotomy" under FISA as enacted in 1978. n213 The overall effect of the opinion was to uphold the Ashcroft Guidelines against statutory and constitutional challenges.

The opinion dismissed the view, adopted by the FISC, that the 1978 version of FISA had contemplated some form of the "wall." n214 The FISCR referred to the "supposed barrier" against information sharing. n215 It said it was "quite puzzling" why the Department of Justice, since at least the 1980s, had read the statute to limit the use of FISA surveillance when intended for criminal prosecution. n216 The court then acknowledged that at least the United States Courts of Appeals for the First, Second, Fourth, and Eleventh Circuits had interpreted FISA to mean that "the primary purpose" of surveillance was supposed to be for foreign intelligence purposes. n217 In finding that all of these cases were incorrect on the doctrine, the FISCR said that it "is almost as if [these cases] assume that the government seeks foreign intelligence information (counterintelligence) for its own sake - to expand its pool of knowledge - because there is no discussion of how the government would use that information outside criminal prosecutions." n218

In my opinion, this quote ignores a commonsense and widely shared alternative view. The alternative approach was explained by the FISC judges, who address foreign intelligence surveillance on a daily basis - the text of the statute refers to the need to "obtain, produce, and disseminate foreign intelligence information." n219 As written in 1978, "the purpose" of the surveillance must be for foreign intelligence information. n220 Once that surveillance also happens to turn up evidence of criminal violations, then that information can be provided to law enforcement officials. n221

[*1338] This alternative explanation is consistent with the legislative history of the 1978 law, which was a compromise between advocates for law enforcement and civil liberties. A vivid concern from the civil liberties side was that the secret FISA wiretaps would expand into an unchecked power to do surveillance outside of the safeguards of Title III. The 1978 House Report clearly indicated the thinking at the time. It stated that "FISA surveillances 'are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it concerns United States persons must be necessary to important national concerns.'" n222 In response to this seemingly clear quotation, the FISCR said only: "That, however, was an observation, not a proscription." n223 To put the matter rhetorically, the FISCR found it "quite puzzling" why the Department of Justice would comply with the "wall," even when multiple circuit courts had thus interpreted the new statute. I find it "quite puzzling" how the court could so easily dismiss the view that FISA was enacted to seek foreign intelligence information, and was not supposed to be a tool for any law enforcement official who wanted to avoid Title III and the other usual restrictions on domestic surveillance.

With that said, I find more persuasive the FISCR's finding that the Patriot Act changed the relevant law for sharing gathered intelligence with law enforcement. The new law stated that "a significant purpose" rather than "the purpose" had to be for foreign intelligence. The court wrote, "Congress was keenly aware that this amendment relaxed a requirement that the government show that its primary purpose was other than criminal prosecution." n224 While correctly finding that Congress intended to change the rules, the court made it surprisingly easy for the government to meet the standard of "a significant purpose." The government need show merely "a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes." n225 The court added, "so long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test." n226 This interpretation of "significant purpose" gives little weight to what is "significant." It especially seems to ignore the decision by Congress to raise the administration's proposed language of "a purpose" up to the stricter test of a "significant purpose." n227

[*1339] The last portion of the FISCR opinion addresses constitutional challenges advanced in amicus briefs submitted by the National Association of Criminal Defense Lawyers and by an alliance of groups led (alphabetically) by the American Civil Liberties Union. n228 It seems quite possible that a court more troubled by civil liberties issues than the FISCR panel would have found the constitutional challenges more compelling under the Fourth Amendment, First Amendment, and Due Process Clause. The FISCR, however, found the challenges without merit. It correctly noted that Keith addressed domestic security, not the constitutionality of surveillance of agents of foreign powers. n229 The court did not, though, address the complex line-drawing issues between domestic and foreign intelligence surveillance that the Supreme Court had noted in Keith. n230 The FISCR also did an overall "reasonableness" assessment of FISA surveillance under the Fourth Amendment in comparison with Title III. n231 In finding that FISA meets constitutional requirements, the court concluded that "in many significant respects the two statutes are equivalent, and in some, FISA contains additional protections." n232 The FISCR panel did not directly address the detailed analysis by the FISC that showed the crucial differences between the two regimes. n233

In summary, the legal changes in the Patriot Act significantly expanded the potential range of searches under the foreign intelligence laws. The revised guidelines in the Department of Justice permit a broader range of domestic security surveillance. The FISCR decision rejected statutory and constitutional challenges to this greatly expanded sharing between foreign intelligence and law enforcement investigations.

V. The System of Foreign Intelligence Surveillance Law

The Article to this point has explored the complex history that led to the 1978 passage of FISA and the 2001 changes contained in the Patriot Act. This Part creates a framework for analyzing the system of foreign intelligence surveillance law. The next Part examines specific proposals for reform.

A. Foreign Intelligence Law as a System for Both National Security and the Rule of Law

One way of understanding FISA is that it substitutes a systemic check on abuse for the case-by-case checks on abuse built into ordinary law enforcement actions. In a Title III case, a neutral magistrate decides whether to authorize a wiretap based on probable cause and other showings required by [*1340] the statute. n234 The target of the wiretap receives notice after the wiretap is complete and has access to the transcripts in order to prepare the defense. n235 The full protections of the American criminal justice system then apply, with rights provided by the Fourth, Fifth, and Sixth Amendments and from other sources. Critics of the current criminal system may believe that additional rights are constitutionally required or statutorily desirable, but the basic approach is one based on individual defendants being able to assert their rights in open court. n236

These individualized protections clearly work less well for FISA cases. Many FISA surveillance orders never result in criminal prosecutions. In those instances, no one outside of the government ever learns about the existence or nature of the surveillance. For those FISA orders that do create evidence for criminal cases, extraordinary procedures prevent defendants from seeing the nature of the evidence against them. n237 For example, the defendant cannot compare an original statement with the translation prepared by the government translator. n238 If the government translator exaggerates the threat in a defendant's statement, through bias or the lack of knowledge of a dialect's nuance, then there is no adversary system to correct the mistake.

Under FISA, a greater share of the safeguards against abuse occur at the system-wide level. System wide, can Congress provide effective oversight of foreign intelligence surveillance? System wide, do Attorney General Guidelines and other Justice Department oversight dictate appropriate checks on the FBI and other intelligence agencies? How well does the OIPR work? Do the judges on the FISC provide helpful judicial supervision of the system, even without an adversary process? Whatever the answers to these questions, it is clear that, compared to criminal procedure, fewer of the safeguards happen at the individual (retail) level, and more happen at the systemic (wholesale) level.

If one considers FISA as part of a system for foreign intelligence law, then the two principal goals of the system are protecting national security and doing so in a manner consistent with the Constitution, the rule of law, and civil liberties. In pursuing these goals, the individual components of the legal system might vary over time or based on differing judgments about efficacy or overall desirability. To give one example, broad surveillance might be accompanied by greater external oversight. An alternative but roughly equivalent approach might have less intrusive oversight but also less broad access to records. To give another example, greater constitutional protections might be accompanied by fewer statutory limits, or fewer constitutional protections might be accompanied by more detailed statutory provisions. In short, there are alternative institutional approaches for seeking the twin goals of national security and the rule of law. The normative goal should be to [*1341] assess the institutional choices to help develop an overall, sustainable system of foreign intelligence law. n239

B. The Special Status of the 1978 Compromise

In considering alternative institutional approaches, I suggest that the appropriate baseline is the 1978 compromise that resulted in passage of FISA. As a matter of constitutional law, the Supreme Court provided its clearest guidance about the Fourth Amendment and electronic surveillance in the period just before 1978. The 1967 Katz and Berger decisions overruled Olmstead and emphasized the strong constitutional limits on how electronic surveillance could be used for law enforcement purposes. n240 The constitutional mandates for law enforcement wiretaps notably included notice to the target once a wiretap was concluded and the ability of defendants to confront the wiretap and other evidence against them. n241 The 1972 Keith case held that the Fourth Amendment requires a prior warrant for electronic surveillance in domestic security matters. n242 While bringing "domestic security" cases clearly within the scope of the Fourth Amendment, Keith expressed "no opinion as to ... activities of foreign powers or their agents." n243 Congress precisely tracked Keith in enacting FISA in 1978 to apply to "foreign powers or their agents." n244 In doing so, Congress legislated in the zone left undefined by the Supreme Court, but did not apply the new FISA procedures to the law enforcement actions governed by Katz and Berger, or to the domestic security matters governed by Keith.

The 1978 compromise responded not only to these constitutional directions from the Supreme Court but also from what one might call the "constitutional moment" of the Watergate events. n245 The magnitude of the constitutional crisis is encapsulated by the resignation of President Nixon, the only such resignation in history. The Church Committee and other revelations of the period, as discussed above, cast unprecedented light on systematic problems in how surveillance was conducted, including: routine violations of law; expansion of surveillance, for preventive and other reasons; secrecy; use against political opponents; targeting and disruption of unpopular [*1342] groups, including the civil rights movement; chilling of First Amendment rights; harm to individuals; distortion of data to influence government policy and public perceptions; issues of cost and ineffectiveness; and the risk of entrenching current leadership. n246

In reaction to new constitutional doctrine and the constitutional magnitude of the Watergate crisis, Congress engaged in the most elaborate deliberation in its history on how to legislate in the linked areas of domestic security, foreign intelligence, and law enforcement. n247 The intelligence agencies and other concerned parties expressed their views to Congress. FISA was a result of these intense deliberations. I believe there should be a burden of proof on those who would substantially change the system of foreign intelligence surveillance law from the 1978 compromise. Proponents of change should explain how proposed changes would be consistent with the Constitution and lead to an overall improvement in the system of foreign intelligence surveillance law.

C. To What Extent Did "Everything Change" After September 11?

Proponents of expanding FISA argue on a number of grounds that "everything has changed" since the attacks of September 11, 2001. n248 President Bush, in his address to Congress nine days later, called for expanded surveillance powers and said, "Americans have known surprise attacks, but never before on thousands of civilians. All of this was brought upon us in a single day, and night fell on a different world, a world where freedom itself is under attack." n249 In considering what may have changed and what may justify legal [*1343] changes, prominent candidates include: the magnitude of the threat; the nature of the threat from terrorism rather than nation states; the domestic component of the threat, including "sleeper cells"; the failure of the previous intelligence system to prevent the attacks of September 11; and the need to respond to new threats more quickly, in "real time." After elaborating on claims that these threats justify greater surveillance powers, the discussion here explains significant counterarguments. n250

1. Magnitude of the Threat

The attacks of September 11 resulted in the highest number of deaths of any foreign attack on U.S. soil. A great deal of government attention has focused since the attacks on the risks of "weapons of mass destruction," including discussion of the risk that terrorists will gain control of nuclear devices. In rhetorical terms, proponents of surveillance can ask: "What limits on surveillance do you want us to observe if we know that someone has a nuclear bomb somewhere in New York City?"

2. Threat from Terrorists Rather than Nation States

During the Cold War, the global landscape was frozen to an extent into pro-Western and pro-communist blocs. The greatest threats came from identified enemies, and the hot line and other institutions were developed for regularizing contacts between the opposing blocs. By contrast, the terrorist threat is inchoate and geographically in flux. In a world of asymmetrical warfare, greater surveillance can detect and respond to newly emerging threats.

3. Sleeper Cells and Other Domestic Threats

The threat today is not principally from foreign states and their hired agents. Instead, the hijackers on September 11 and the detection of a possible sleeper cell in Lackawanna, New York show that serious threats exist here at home. n251 Given the proven size of terrorist attacks, the emphasis must be on prevention of attacks before they occur. n252 Extensive surveillance before the commission of any crime is needed to achieve that prevention.

4. The Failure of the Previous Intelligence System

A law professor is tempted to say "res ipsa loquitur." The attacks of September 11 happened, and what more needs to be said about the need to [*1344] change the previous system for antiterrorist intelligence gathering? In particular, the failure of the FBI and the CIA to "connect the dots" - caused in no small part by the "wall" that prevented information sharing - meant that key information in Moussaoui's computer was not read until after the attacks. n253 In the face of this crucial failure, the burden has been met for shifting to greater information sharing and preventive action.

5. The Need to Respond in "Real Time"

Terrorists today communicate at the speed of the Internet. Al Qaeda has a flexible, global network to respond quickly and unpredictably to new opportunities for terrorism. In responding to these fast-moving threats, American intelligence agencies cannot afford to be slowed down by burdensome warrants and other paperwork requirements. Information must be shared in real time with the officials who need it, so that responses can match the nature of the threat.

D. Some Responses to the Claim that "Everything Has Changed"

Anyone considering this list of risks - the magnitude of the threat, its terrorist nature, the domestic threats, the previous failures, and the need to respond in real time - should seriously consider the possibility that important changes to the 1978 compromise are now due. The acts of our national leaders underscore the concern. Attorneys General Reno and Ashcroft, who disagree on many issues, both made fighting terrorism a priority. Antiterrorism funding and the number of FISA orders increased rapidly under President Clinton, n254 and President George W. Bush has made fighting terrorism a centerpiece of his administration's policies.

The difficult judgment, especially for anyone who does not have access to classified information about actual threats, is to assess the magnitude of the risks to national security and the effectiveness of surveillance powers to reduce those risks. This Article earlier showed reasons for believing that historically there has been excessive domestic surveillance against "subversives" and other domestic threats, but the risks facing the country today may be greater. Henry Kissinger is credited for the quip: "Even a paranoid has some real enemies." n255 The U.S. intelligence agencies are paid to be paranoid, to consider any possible threats against the nation. Even if they have sometimes exaggerated the risk in past periods, the risks today or the effectiveness of new surveillance tools may justify stronger surveillance measures. In addition, [*1345] after the revelations of the 1970s, the watchdog capabilities of the press and the public may be greater, so that the risk of abuse may be lower now.

This uncertainty about the actual threats argues for a particular humility in recommending how to legislate on foreign intelligence surveillance when the current FISA provisions expire in 2005. Nonetheless, there are significant counterarguments to the claim that "everything is different."

1. The Magnitude and Non-Nation State Nature of the Threat

There is a natural human tendency to feel that the problems of the moment are particularly severe, yet the size of the terrorist threat seems smaller when seen in historical context. The most relevant historical comparisons are likely to the Palmer Raids after World War I, McCarthyism in the early 1950s, and the civic disturbances of the Vietnam era. n256 The Palmer Raids and McCarthyism were direct responses to the fear of international communism. n257 The timing of those periods of anti-communism was no accident. Each closely followed on a major communist success - the Bolshevik Revolution of 1917 and the triumph of Mao in China in the late 1940s. n258 Compared with capturing the two largest countries in the world, nothing in the terrorist list of accomplishments comes close. The threat from the civic disturbances of the late 1960s and early 1970s is more difficult to quantify. At the sheer level of disturbance of daily life, however, the disruptions were clearly greater then than now. Most major cities suffered riots during this period and the Keith Court itself, while upholding the Fourth Amendment requirement for domestic surveillance, noted government statistics that there were 1562 bombing incidents in the first half of 1971 alone, most of which involved government-related facilities. n259

It is also questionable to assert that there is greater threat from terrorists than from an enemy nation state. At the level of logic, it seems likely that a large, well-organized enemy with a secure territory (i.e., a nation state) will pose a greater threat than a dispersed enemy that lacks a physical safe haven. That is why there is such emphasis on inhibiting the state sponsors of terrorism. At the historical level, the McCarthy period coincided with the demonstration that the Soviets had developed the atomic and then the hydrogen bomb, as well as a large-scale conventional war with the North Koreans and then the Chinese. n260 With the development of the intercontinental ballistic missile, the enemies of the United States developed the clear capacity to wipe out many American cities and perhaps all human life on Earth. n261 By comparison, the terrorist threat today, as severe as it is, is less all-encompassing.

[*1346]

2. The Threat Domestically

Many Americans today are struck by the insidious, domestic nature of the terrorist threat. The hijackers of September 11 lived in ordinary neighborhoods and carried out many commonplace daily activities. A member of a sleeper cell might be just down the block from your home at this moment. Faced with these agents of foreign interests acting at home, surely the special nature of this threat calls for new, strong measures.

In response, history shows that the earlier periods of high surveillance also involved threats that Americans believed were dangerously domestic yet linked with foreign influence. The Palmer Raids were directed in large measure at new immigrants from Eastern Europe who were suspected of being sympathetic to international Bolshevism. n262 In the 1950s, the fears stereotypically were of a communist under every bed; more soberingly, historians today generally accept that Alger Hiss and other senior American officials indeed were spying for the Soviet Union, and a large number of Americans were linked with organizations that can now be identified as communist fronts. n263 J. Edgar Hoover's relentless surveillance of Martin Luther King, Jr. during the 1960s seems to have been based in part on his belief that King was a communist. n264 As the Vietnam War progressed, U.S. intelligence agencies continually tried to link domestic political opposition to communist and other foreign influence. n265 This history does not discount the domestic threat, but it shows that domestic risk has been a staple of previous periods rather than being a new phenomenon of September 11.

3. The Failure of the Previous Intelligence System

There is no brief answer to the question of whether the attacks of September 11 demonstrate a failure in the previous rules for foreign intelligence. In many ways, the inquiry into the proper system of foreign intelligence is the subject of this entire Article. A few points, however, can cast doubt on the res ipsa loquitur idea that the existence of the September 11 attacks demonstrates a need for substantial change in the legal framework directing surveillance. First, publicly available information shows that the FBI and other intelligence agencies had successfully detected and halted attacks before September 11. n266 These successful actions provide context for the failure to prevent the September 11 attacks. Second, the failure to gain timely access to Moussaoui's computer seems to have resulted in part due to the FISC concerns [*1347] that FISA applications had become misleading. n267 Accurate applications, rather than a wholesale change in the law, could be a sensible response to that sort of problem. Third, the Coleen Rowley whistleblowing indicates a variety of other problems within the intelligence system that could be solved without the need for enhanced surveillance powers. n268 Fourth, it is far from certain that the weaknesses of the system before September 11 resulted from an insufficiency of surveillance and other powers to gather information. Much of the criticism of the system, according to congressional hearings, seems to be a lack of analysis rather than a lack of information. n269 For instance, there apparently was a large backlog of FISA intercepts that were not translated and analyzed in a timely fashion. n270 In such a setting, increased surveillance can lead, colloquially, to adding more hay to the haystack. Making the haystack bigger makes it no easier to find the needle.

4. The Need to Respond in "Real Time"

There are at least two categories of responses to the claim that the need to respond more quickly makes "everything different" now. A factual basis for questioning whether everything has changed is the observation that the perils facing the nation feel urgent in every age. Consider the situation facing intelligence officials during the war against Hitler's Germany or in the midst of the Cuban missile crisis. In every age, it will be the rare official who says "our problems today are not very urgent, so we can use slow means for making intelligence assessments." The need for speed feels imperative in the midst of every crisis.

Fortunately, as a legal matter, FISA has always permitted emergency wiretaps. n271 Such wiretaps are now permitted if the Attorney General reasonably determines that an emergency situation requires surveillance to begin "before an order authorizing such surveillance can with due diligence be obtained." n272 An application is then made to a judge in the FISC "as soon as practicable, but not more than seventy-two hours after the Attorney General authorizes such surveillance." n273 This provision creates a legal basis for responding in real time under the current statute, with prompt judicial oversight. The number of emergency FISA orders has increased sharply since [*1348] September 11. More than 170 emergency FISA orders were issued in the eighteen months after the attacks, three times the number authorized in the first twenty-three years of the statute. n274 In short, the need to respond quickly is felt imperative in every age, and the emergency FISA wiretaps provide a legal route to respond quickly.

E. Considerations Suggesting Caution in Expanding Surveillance Powers

Before turning to proposals for reform, it is useful to discuss two considerations that suggest caution in believing that expanding surveillance powers is appropriate: the "ratcheting-up" effect, and the likelihood that long-term preferences for privacy protection are greater than short-term preferences.

The "Ratcheting-up" Effect. There are substantive and public choice reasons that lead to a "ratcheting up," or increase, in surveillance authorities over time. n275 This ratcheting-up effect stems in part from the complexity of electronic surveillance law. Although this Article has focused on the differences between Title III and foreign intelligence surveillance, a complete account of wiretap and electronic surveillance law requires the description of numerous other distinctions. For instance, legal standards vary for: "wire" or "oral" versus "electronic" records; content of communications versus pen register information; "interception" of communications versus access to stored records; and short-term versus long-term stored electronic communications. n276

As a substantive matter, this complexity leads to numerous possible analogies for why surveillance powers should be expanded. We have already seen examples in the FISA context. Although the 1978 law provided only for surveillance of the content of electronic communications, Congress gradually expanded FISA to other tools commonly used in law enforcement, such as physical searches, pen register and trap and trace orders, stored records and other tangible things. n277 For each example, one can readily imagine the policy argument - we allow these searches for ordinary crimes, even low-level drug crimes, so shouldn't we be able to have the same powers when fighting terrorism and protecting national security? n278 This "ratcheting-up" effect is [*1349] in addition to a more general reason why surveillance powers expand over time: intelligence agencies get part of a picture but are unable to understand the entire picture and thus seek and receive additional powers, with the hopes that the additional surveillance capabilities will be more effective at meeting the goal of preventing harm before it occurs.

The potential persuasiveness of these arguments for expansion is given greater effect due to the institutional or public choice realities of how surveillance legislation is enacted. The basic dynamic is that there are lawyers and other experts in the Justice Department and the intelligence agencies whose daily job is to work with the intricacies of the surveillance law. These professionals encounter obstacles in their daily work and develop proposed legislation to remove these obstacles. In many years these proposals for increased surveillance powers will not pass Congress due to general concerns about civil liberties. When a crisis hits, however, there are strong pressures to "do something" to respond to the threat. At that instant, the dormant legislative proposals come out of the drawers. Legislation that would not otherwise be enacted thereby becomes law.

The clearest example of this phenomenon is the Patriot Act itself, which the Bush administration introduced to Congress just six days after the attacks of September 11. n279 The great majority of the new surveillance provisions had been discussed within the executive branch or Congress in previous years and had not been adopted. n280 After the September 11 attacks, professional staff in the agencies simply went into their files and pulled out provisions they had been advocating previously. In the super-charged climate of the fall of 2001 many of these provisions received remarkably little scrutiny or public debate. This same pattern of suddenly enacting surveillance powers after an attack had happened before, such as in the wake of the Oklahoma City bombing. n281 In recognition of this pattern of ratcheting up, an extra note of caution is appropriate before concluding that an additional round of broader surveillance powers is appropriate.

[*1350] Short-Term and Long-Term in Privacy Protection. The ratcheting-up effect is an example of a broader phenomenon in privacy law, the gap between short-term and long-term preferences. As I have previously discussed for private-sector privacy, n282 in the short run, faced with a modest advantage in convenience or cost, individuals are often willing to disclose some of their personal information to companies. n283 In the long run, by contrast, many individuals strongly prefer a society characterized by significant privacy compared with a society characterized by pervasive disclosure and lack of privacy. n284 One indication of this long-term preference is a Wall Street Journal poll in late 1999 asking Americans what they feared most in the coming century. Among a dozen answers, such as nuclear holocaust and global terrorism, the most frequent answer was "loss of personal privacy." n285

A similar tension exists in views towards additional surveillance. In the short term, when asked whether they would support a specific measure to fight terrorism, many people would support the measure. Support for new security measures would be especially high in the midst of a crisis. On the other hand, especially as the crisis eases, many people would then support overall measures that reduce the risk of a "Big Brother" society. The "ratcheting-up" effect and the likely long-term preferences of the public for greater privacy protections fit together with the reasons developed above why "everything has likely not changed." They all provide reasons for skepticism about whether greater surveillance should be authorized.

VI. Proposals for Reform

In light of the discussion above of the history and structure of foreign intelligence surveillance law, we are now in the position to assess proposals for reform. Much of the discussion here will be on proposals that enhance the checks and balances in the system of foreign intelligence surveillance law. Considering such proposals is the role of Congress and others outside of the executive branch who seek to shape an overall system that will meet today's national security goals while also creating effective long-term ways to protect the rule of law and civil liberties.

Perhaps less obviously, proposed reforms may also strengthen the practical ability of the foreign intelligence agencies to accomplish their national security mission. The passage of FISA in 1978, for instance, regularized the use of foreign intelligence wiretaps and thus almost certainly enabled a larger number of such wiretaps than would have existed under the President's inherent authority to protect the national security. Conversely, the absence of legal standards creates the possibility that surveillance will take forms that, once exposed, lead to harsh limits on the future ability to conduct wiretaps and other information gathering. In the short-term the officials charged with [*1351] running the system will rarely volunteer to subject themselves to greater oversight or stricter legal rules. In the long-term, however, a system operating under the rule of law may well be less prone to embarrassing excesses and possibly punitive reactions from Congress and the general public. n286

The issues of reforming the system are not partisan. In thinking about what long-term system should exist, I invite the reader to consider whichever Attorney General in recent decades that the reader has trusted the least. It is well known, for instance, that many Republicans expressed concerns about excessive Justice Department actions under Attorney General Reno, such as during the Waco incident. Many Democrats have expressed concerns about excessive surveillance by the Justice Department under Attorney General Ashcroft. Once one has that least-trusted Attorney General in mind, whomever it may be, the job for system design is to create rules and institutions that will survive eight or more years of that sort of leadership. There is little need for checks and balances if one entirely trusts the executive. The goal is a long-term system that will have checks and balances that are effective enough to survive periods of emergency or the temporary tenure of officials who seek to use excessive surveillance.

This Part will group possible reforms into five somewhat overlapping categories: (1) the practical expansion of FISA since 1978; (2) section 215 and NSL powers to get access to records and other tangible objects; (3) what to do about "the wall" between criminal and foreign intelligence investigations; (4) reforms to the FISC system; and (5) ways to address the long-term secrecy of the FISA system. The effort here is to suggest a number of potential ways to improve the system rather than to insist that a few specific proposals are clearly desirable. Greater oversight of the system is needed, and a first use of the analysis in this Article could be to assist in framing oversight inquiries. In light of the twin goals of protecting national security and upholding the rule of law, practical judgments will need to be made about which of the various reform proposals fit best together. The very significant changes since 1978, however, lead me to believe that a new set of checks and balances is almost certainly needed to replace the legal and practical limits that have fallen away over time.

A. The Practical Expansion of FISA Since 1978

A brief review of history shows the practical expansion of FISA since 1978, and points the way to possible reforms. Without intending to idealize the situation at that time, by the late 1970s a system of interlocking safeguards existed against excessive surveillance. The Supreme Court had recently decided Katz, Berger, and Keith, showing its concern for constitutional standards in law enforcement and domestic security cases. n287 The Levi Guidelines protected against intrusions into First Amendment activities. n288 At a practical level, the early version of the "wall" limited the extent to which [*1352] foreign intelligence surveillance was used as a routine tool of law enforcement. n289 The vivid memory of the Watergate revelations meant that the press, the Congress, and the members of the intelligence community all knew at a personal level the problems that could arise from excessive surveillance. The level of foreign intelligence surveillance was also at a relatively small scale, with 319 applications presented in 1980. n290

The situation today is quite different. In the federal courts, the 2002 FISCR decision suggests few constitutional limits on FISA surveillance (although I believe that strong constitutional arguments exist against that decision). n291 The Levi Guidelines have given way to the 2002 Ashcroft Guidelines, which far more aggressively contemplate surveillance of First Amendment activities in the name of domestic security. The "wall" has come down entirely, to the extent that prosecutors can direct and control investigations that use FISA surveillance. n292 The memories of the 1970s have faded, with many veterans of that period having retired and with the pressing emergency of Al Qaeda seeming to many to make that history inapposite. The number of FISA applications jumped to 1228 in 2002, and Attorney General Ashcroft has announced his intension to use FISA powers extensively in law enforcement actions. n293 The extension of FISA to any documents or tangible objects, and the accompanying rules preventing public disclosure of such searches, creates a legal structure for thoroughgoing secret surveillance of many domestic activities. In short, the extraordinary power of the President and Attorney General to conduct "national security" surveillance has become far more routine.

1. Expand Reporting on FISA Surveillance

One response to the known expansion of FISA surveillance is to seek greater congressional and perhaps public knowledge of the scope of FISA activities by increasing the reporting requirements. The logic behind increased reporting is that greater oversight is needed where there is increased surveillance and potential infringement of civil liberties.

The current level of FISA reporting is considerably less than exists for Title III wiretaps or pen register and trap and trace orders. n294 For FISA, the public reports only give the annual number of applications made for electronic surveillance and the number of such orders granted, modified, or denied. n295 [*1353] The Attorney General also reports semiannually to the House and Senate Intelligence Committees with a description of "each criminal case in which information acquired under [FISA] has been passed for law enforcement purposes" and for "each criminal case in which information acquired under [FISA] has been authorized for use at trial." n296

Greater reporting is required for pen register and trap and trace orders, which target to/from information, such as the telephone numbers a person calls. These reports include the number of investigations involved, the offense specified in the order or application, and the identity of the applying investigative or law enforcement agency. n297

Even more detailed reporting is required for Title III orders, which target the content of communications and are thus more intrusive than pen register orders. For each order, the judge submits a report to the Administrative Office of the United States Courts that includes: the fact the order was applied for; whether the order was granted, modified, or denied; the period of interceptions authorized as well as any extensions; the offense specified in the order; the identity of the applying officer and agency as well as the person authorizing the application; and the nature of the facilities from which communications were to be intercepted. n298 Annually, the Attorney General must make an additional report to the Administrative Office of the United States Courts. This report includes the information submitted by the judges as well as a general description of the interceptions made under an order. The general description is supposed to include: the approximate nature and frequency of incriminating communications intercepted; the approximate nature and frequency of other communications intercepted; the approximate number of persons whose communications were intercepted; the number of orders in which encryption was encountered and whether such encryption foiled the investigation; and the approximate nature and cost of the manpower and other resources used in the interceptions. n299 The Attorney General is also supposed to report on: the number of arrests resulting from interceptions; the offenses for which arrests were made; the number of trials resulting from such interceptions; statistics on motions to suppress; and the number of convictions resulting from such interceptions. n300 The Administrative Office of United States Courts releases an annual report that gives statistics [*1354] on the number of orders as well as a summary and analysis of the detailed data provided by judges and prosecutors. n301

The more detailed reporting available on Title III orders may prove a useful model for expanded reporting for FISA orders. There are conflicting intuitions on whether greater reporting is appropriate for FISA. On the one hand, there is the tradition of secrecy for foreign intelligence activities. More detailed reporting might reveal the advanced sources and methods deployed for the most sensitive foreign intelligence investigations. It might also allow inferences about the level of surveillance of embassies and embassy personnel, potentially leading to diplomatic embarrassment. On the other hand, statistical reports about Title III are less important because the target of the surveillance learns about the wiretap after it is ended. With a FISA order, that individualized notice of the nature of the surveillance is absent, and systemic reporting thus becomes more important. Without systemic reporting, it will be difficult to learn if the extraordinary powers of FISA are being used in new and potentially disturbing ways.

My own judgment on additional reporting is that the topic should at least be the subject of congressional attention and oversight. The reporting used for pen registers and Title III provides a useful list of candidates for additional FISA reporting. Some categories of reporting could be made available to the public, while more sensitive categories of information might be supplied only to Congress. The strongest case for additional public reporting may be for criminal prosecutions that result from FISA orders. In such instances, defendants face unique difficulties in presenting their cases, likely including the inability to examine the surveillance tapes and other evidence used against them. There is thus special reason to keep the general public informed about the scope of FISA prosecutions.

2. Defining "Agent of a Foreign Power"

Comments I have heard in public from knowledgeable persons suggest that there has been ongoing expansion of who is considered an "agent of a foreign power." n302 Consider an individual who works in the United States for the Cali drug cartel. Is that person an "agent of a foreign power?" The Cali cartel is a highly organized group that physically controls a substantial amount of territory in Colombia. n303 Given these facts, one might well argue that the Cali cartel is more of a "foreign power" than the amorphous Al Qaeda network. If one accepts the Cali cartel as a "foreign power," and a major smuggler as an "agent of a foreign power," would a street-level cocaine dealer also qualify as its agent? There is no clear line in the statute stating that the dealer would not be so considered. To take another example, what about the activities of the so-called "Russian mafia"? Many organized crime [*1355] groups have links to overseas operations. How small can the links back home be to still qualify that group's actions as on behalf of a foreign power?

These examples, it turns out, go to the heart of whether Title III will continue to be a significant part of the overall American system of electronic surveillance. The threat of organized crime was a principal justification in 1968 for the extraordinary intrusion of performing wiretaps under Title III. n304 Over time, narcotics and organized crime cases have constituted the vast bulk of federal Title III wiretaps. In 2002, for instance, narcotics cases numbered 406 (81%) and racketeering cases numbered 59 (12%) out of the 497 total federal wiretaps. n305 Yet an expansion of the definition of "agent of a foreign power" could render Title III wiretaps almost obsolete. Many heroin, cocaine, and other drug cases are linked to imported narcotics. Many organized crime cases in this era of globalization have significant links to overseas activities. FISA orders already outnumbered Title III orders in 2003. n306 If most drug cases and organized crime cases shift to the secret world of FISA, then the constitutional teachings of Katz and Berger may have little effect.

In debates about U.S. wiretap law there is often an implicit assumption that Title III wiretaps are the "normal" means of surveillance, with FISA orders as an exception used for embassies and other foreign intelligence functions. The available statistics, however, show that in 2002 the federal government secured 497 Title III orders, compared to 1228 FISA orders. n307 Title III orders were thus only 28.8% of the total for that year. One cannot tell from publicly available information how far the government is already moving toward using FISA orders for narcotics and organized crime investigations within the United States. It is possible that many such cases already use FISA orders. It is also possible that an expanded definition of "agent of a foreign power" will mean that more such cases will be handled under FISA in the future. Because of the lesser constitutional and statutory protections existing in FISA investigations, Congress should use its oversight powers to learn more about the contours of what it takes for someone to be considered an "agent of a foreign power."

If this oversight shows that "ordinary" drug and organized crime cases are becoming foreign intelligence cases, then various reforms may be appropriate. One approach would be to require reporting concerning whether a Title III order would have been available for the investigation. A stricter step would be to introduce a prohibition on FISA use where Title III would suffice. A different approach would be to tighten the definition of "agent of a foreign power" to delineate when ordinary constitutional and Title III requirements [*1356] would apply. In the absence of public knowledge about how the definition of "agent of a foreign power" is now interpreted, however, it is difficult to know what reforms, if any, are appropriate.

B. Section 215 and National Security Letter Powers to Get Records and Other Tangible Objects

The Patriot Act substantially expanded the government's power to obtain records and other tangible objects through section 215 and NSLs. The expanded scope of these powers is controversial for two distinct reasons - the potentially routine use of foreign intelligence powers to seize any records, and the "gag rule" that makes it a federal crime for the holder of the record to tell anyone, even the press, about the seizure.

1. Expanding the Use of National Security Letters

As discussed above, n308 NSLs were expanded in section 505 of the Patriot Act in the following ways: they no longer are limited to counterintelligence operations; the relatively strict requirement of "specific and articulable facts" that the information pertain to an agent of a foreign power was lowered to the looser "relevant to an investigation" standard; records about persons other than agents of foreign powers are thus now subject to NSLs; and a "Special Agent in Charge" at an FBI branch office can authorize the NSL, rather than requiring approval from a more senior official at FBI headquarters. As discussed further below, NSLs also are subject to the "gag rule" prohibiting disclosure of the NSL by the record holder. n309

From the perspective of checks and balances, these expansions of NSLs leave many gaps. Most prominently, NSLs are implemented without judicial supervision. That lack of supervision, combined with the possibility of issuing an NSL without approval by FBI headquarters, creates the possibility of excessive surveillance by field offices. There appears to be no current statutory requirements of any recordkeeping about the use of NSLs. For example, there is no reporting of the annual number of NSLs in the yearly FISA reports to Congress. To address these concerns, possible reforms of the NSL authority and section 215 provisions on record searches are discussed in the next section.

2. Using FISA To Obtain Records and Other Tangible Objects

As discussed above, n310 the Patriot Act expanded the scope of FISA orders to records in important ways: the order can extend beyond travel records to "any tangible things (including books, records, papers, documents, and other items)"; the legal standard was lowered to merely being part of "an authorized investigation"; and the records may be those of any person, rather than requiring "specific and articulable facts that the person to whom the records pertain is a foreign power or an agent of a foreign power." n311 One [*1357] consequence of the statutory change is the apparent permission of a FISA order to encompass entire databases, rather than the specific records of the target of an investigation.

Section 215 has drawn the greatest attention due to the law's potential to obtain library records. n312 The library records controversy is significant in its own right as a debate about whether government should have access at all to First Amendment materials. Government surveillance of reading smacks of the "Thought Police" and the worst fears of "Big Brother" government. Standard First Amendment jurisprudence recognizes the chilling effect on expression and political activity that can result from such surveillance. n313 One specific reform proposal, therefore, would be to exempt library records from the scope of section 215.

The library records controversy is even more important because the same rules apply under section 215 to library and all other records. Section 215 appears to override a wide array of existing laws that limit government access to personal information. For example, existing procedures govern government access to medical records,n314 financial records, n315 and many other categories of records. n316 The medical privacy rule specifically allows disclosure to the government for intelligence investigations and for reasons of national security, n317 and the financial privacy laws allow delay of notice to the target of an investigation upon proper showings. n318 These procedures were crafted after attention to the special sensitivity and other characteristics of each category of record. Section 215, by contrast, is a blunt instrument that allows a single order to give access to all records that the government seeks as part of an investigation.

In response to public concern about use of section 215 to gather library records, Attorney General Ashcroft reported in September 2003 that the section had never been used since passage of the Patriot Act for library or any other records. n319 This lack of usage is reassuring because it shows that the Justice Department has not been using the new power for routine surveillance of library and other sensitive records. The lack of usage also supports [*1358] the position that the Justice Department has not made the case for renewing section 215 when the sunset expires. There are existing procedures for gathering records without using the extraordinary scope of section 215. Absent some new showing by the Justice Department of the specific circumstances where section 215 is needed, the provision should be allowed to sunset.

It is possible that the explanation for the lack of use of section 215 has been the expanded use of NSLs. NSLs are narrower in scope than section 215 orders, because NSLs only apply to specified communications and financial records. n320 NSLs are more worrisome from a civil liberties perspective, however, because of the lack of the judicial supervision that exists with a section 215 order. n321 Oversight is appropriate for NSLs and section 215 orders together, in order to determine what factual settings are fitted to each tool. At a minimum, there should be reporting on the use of NSLs and section 215, as has been suggested already in Congress. n322

In terms of other possible reforms, probing questions are appropriate to determine whether and in what circumstances NSLs and section 215 orders are necessary at all. If the decision to keep some form of NSLs and section 215 is made, however, then there are various reforms that would cabin some of the most disturbing aspects. For instance, there could be a specific carve-out from section 215 for library records. There could be deference to the medical, financial, and other privacy laws on the books, so that the specific statutes would govern categories of records rather than using the lower standard of section 215. Next, the standard for NSLs and section 215 could return to the "specific and articulable facts" standard that existed before 2001, rather than leaving unchecked access to records that simply are part of an investigation. In addition, there could be minimization rules to assure the FISC that only records reasonably necessary to an investigation are sought by the government, rather than all records held by a library or other organization. In crafting minimization rules, possible procedures and promising new technologies could allow government access to the target's documents without turning over the entire database to the government. n323

The overarching concern with NSLs and section 215 orders is the legal authorization for dragnets of entire databases. These searches can remain secret because notice is never given after the fact, and because the "gag rule" [*1359] prevents the record-holders from revealing the existence or scope of the searches. Section 215 sunsets in 2005 but the expanded NSL powers do not. The nature and uses of these two provisions deserve careful attention in any Patriot Act reauthorization.

3. The Unjustified Expansion of the "Gag Rule"

An especially troubling aspect of NSLs and section 215 is the provision that makes it illegal for individuals or organizations to reveal that they have been asked by the government to provide documents or other tangible objects. n324 It appears that the law makes it criminal for a librarian or other person even to say that there has been a FISA request, without saying more about the nature of the request or the name of the target. This "gag rule" is an unjustified expansion of a special rule for wiretaps, and is contrary to the rules that have historically applied to government requests for records.

There has long been a specialized rule for wiretaps, under both Title III and FISA, that the telephone company and others who implement the wiretap are required to keep the wiretap secret while it is in operation. n325 The need for secrecy flows specifically from the recognition that the ongoing usefulness of the wiretap will disappear if its existence becomes known. Indeed, the special nature of ongoing surveillance is the primary reason why the Supreme Court exempted law enforcement wiretaps from the prior notice requirement of the Fourth Amendment, subject to the strict requirement of notice to the target after the wiretap is concluded. n326

This secrecy requirement for those implementing the wiretap is entirely different than the legal rules that apply to ordinary government investigations. Suppose that a landlord is interviewed by police about the whereabouts of a tenant or a company is asked for records about its sales to a particular individual. The American approach in such instances is that the landlord or the company is permitted to talk about the investigation with the press or other persons. This ability to speak to the press or others is an important First Amendment right. Under the "gag rule" approach, that right is taken away and individuals subject to excessive searches must risk criminal sanctions to report overreaching or abuses of government authority.

The general American approach also places key limits on what a landlord or company may say. If a landlord tips off a tenant that the police are trying to catch the tenant, then the landlord is subject to punishment under obstruction of justice or similar statutes. This kind of targeted criminal sanction permits citizens to keep watch on possible overreaching by the government, while also empowering the government to punish those who assist in criminal activity.

The furor about FISA access to library and other records is based in part on the recognition that this sort of broad search power could expand over time into a routine practice of intrusive domestic surveillance. The combination of this essentially unlimited search power with the "gag rule" means that [*1360] the most basic check against abuse - publicity - is removed. Similar "gag rules" have recently spread into other statutes. n327 Instead of multiplying these suppressions on speech, a far better approach is to have a focused inquiry on whether there are gaps in the obstruction of justice or similar laws. My recommendation is that the special circumstances that justify the "gag rule" for ongoing wiretaps do not apply to records searches such as those under section 215 and the NSLs. Records searches are not typically ongoing in the same way as wiretaps, and they generally do not involve the sources and methods that have been so important to surreptitious electronic surveillance. Agents who make the records request can inform the record holder about obstruction of justice and other potentially relevant statutes. n328 The law should be generally clear, however, that disclosure is permitted absent the special circumstances of assisting the targets of investigation.

If that recommendation is not adopted, however, then there are measures that can reduce the risk of ongoing, extensive, and secret searches of records held in the private sector. For instance, there could be a six-month time limit on the prohibition on disclosure, subject to a request to the FISC that a longer duration is necessary. There could be rules about the scope of disclosure, with permission perhaps to report the mere existence of a request without authorization to disclose the nature of the request. That approach could calm the concerns expressed by librarians, for instance, that they could not even report to the American Library Association the number of requests that had been made. Similarly, disclosure might be permitted where the record holder reasonably believes that the disclosure would not reveal information detailed enough to materially assist the targets of an investigation. That approach might permit a large telephone company or Internet Service Provider, for instance, to reveal the number and type of searches without tipping off any targets that they had been the subject of an investigation. n329

C. What To Do About the "Wall"

Much of the recent FISA debate has concerned the extent to which "the wall" should exist between foreign intelligence and law enforcement investigations. n330 [*1361] The following discussion explains the contrasting positions, shows the dilemma they pose, and proposes a different statutory approach to resolve the dilemma.

1. The Logic of the Conflicting Positions

There is great fervor and strong logic on both sides of the debate. Those who want maximum coordination of foreign intelligence and law enforcement stress four arguments. First, the sort of terrorism, espionage, and sabotage detected in foreign intelligence investigations are themselves often crimes, and it frustrates the basic mission of law enforcement to prevent this evidence from being used in criminal prosecutions. Second, prosecution for crimes can lead to arrest and imprisonment. This incapacitation is a powerful tool to disrupt ongoing terrorist operations. Third, the original FISA in 1978 included procedures for using FISA information in criminal cases, so there is historical precedent for information sharing. Finally, the events leading up to September 11, and especially the failure to find and use the information in Moussaoui's computer, show the urgent need to share information promptly between foreign intelligence and law enforcement investigations.

The principal argument on the other side is that criminal prosecutions should be based on the normal rules of criminal procedure, not on evidence gathered in a secret court system. The norm should be the usual constitutional protections rather than the exceptional circumstances that arise in foreign intelligence investigations. Notably, the Fourth Amendment creates a baseline where targets of investigations should receive notice of government searches, either at the time of the search or as soon as practicable afterwards in the case of wiretaps. The Sixth Amendment creates a norm that defendants should confront the witnesses and evidence against them, yet the FISA procedures limit defendants' ability to cross-examine the evidence. The First Amendment should provide assurances of freedom of thought and of the press, without the chilling effect of having "an FBI agent behind every mailbox." n331

From this perspective, "the wall" serves essential purposes. First, despite the FISCR's holding to the contrary, removal of "the wall" may violate the Constitution for investigations that are primarily not for foreign intelligence purposes. At some point an investigation is so thoroughly domestic and criminal that the usual Fourth Amendment and other protections apply. Future review in other courts may find that investigations that are not primarily for foreign intelligence purposes do trigger constitutional protections. Second, "the wall" may be important in preventing the spread of the secret FISA system over time. As of 2002, seventy-one percent of the federal electronic surveillance orders were FISA orders rather than Title III orders. n332 The Patriot Act reduction of safeguards in the FISA system means that this figure may climb in the future.

[*1362] Third, ongoing expansion of the definition of "agent of a foreign power" may mean that an ever-increasing proportion of investigations might be shoehorned into the FISA formula. This shift may exist due to a general trend toward transnational relationships in an era of globalization. It may also exist under pressure to authorize FISA orders even in the case of slight and speculative links to Al Qaeda or other terrorist organizations. Fourth, the history described in Part I above shows the risks of abuse that come with an expanding, secretive system of surveillance that is justified by national security and the fear of subversion. In short, the concern is that the American system of the Bill of Rights could become a secret surveillance system where defendants do not learn of the surveillance and do not confront the evidence against them.

2. Framing the Current Dilemma

The conflicting positions create an apparent dilemma - "the wall" is necessary to avoid the slippery slope into a pervasive secret surveillance system, but "the wall" prevents necessary coordination of law enforcement and foreign intelligence in the war against terrorism. A particular problem is that, early in an investigation, it may be difficult or impossible for investigators to know whether the evidence will eventually be used for intelligence purposes or in an actual prosecution. For instance, imagine that a FISA wiretap is sought for a group of foreign agents who are planning a bomb attack. On these facts, there would be a strong foreign intelligence purpose, to frustrate the foreign attack. In addition, there would be a strong law enforcement basis for surveillance, to create evidence that would prove conspiracy beyond a reasonable doubt. On these facts, it would be difficult for officials to certify honestly that "the primary purpose" of the surveillance was for foreign intelligence rather than law enforcement. The honest official might say that the surveillance has a dual use - both to create actionable foreign intelligence information and to create evidence for later prosecution.

Faced with this possibility of dual use, the Patriot Act amendment was to require only that "a significant purpose" of the surveillance be for foreign intelligence. Under the new standard, an official could honestly affirm both a significant purpose for foreign intelligence and a likely use for law enforcement. The problem with the "significant purpose" standard, however, is that it allows too much use of secret FISA surveillance for ordinary crimes. The FISCR interpreted the new statute in a broad way: "So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test." n333 The range of "realistic options" would seem to be so broad, however, that FISA [*1363] orders could issue for an enormous range of investigations that ordinarily would be handled in the criminal system. For instance, "realistic options" for investigators would include: continued surveillance of the target; using surveillance of this target to learn more about possible associates; and efforts to "turn" the target into an informer. These techniques are the bread and butter of criminal law enforcement. Under the language of the FISCR opinion, any of these "realistic options" would appear to be enough to justify a FISA order. The Patriot Act amendment, as interpreted by the FISCR, thus allows the slippery slope to occur. A potentially immense range of law enforcement surveillance could shift into the secret FISA system.

3. Resolving the Dilemma by Focusing on the Foreign Intelligence Value of the Surveillance

To resolve the dilemma, the proposal here is to focus on the appropriateness of an application as a foreign intelligence investigation, rather than seeking to measure the amount of dual use for law enforcement purposes. The essential goal is to issue FISA orders when they are "worth it" for foreign intelligence purposes. The previous approaches, based on "primary" or "significant" purpose, suffer the defect that it is difficult to guess at the beginning of an investigation whether a FISA order will result in evidence of a crime, foreign intelligence information, or both. The better approach is to ask those seeking the FISA order to certify that the extraordinary, secret surveillance order be used where there is a significant foreign intelligence reason for the order.

To achieve this goal, some new statutory language would need to be added to FISA. Under current law, an order may issue where there is probable cause that the person under surveillance is an "agent of a foreign power."n334 As discussed above, n335 this standard has become too minimal in today's transnational environment, where the term "foreign power" can apply to so many nonstate actors and where "agent of a foreign power" might extend to a large fraction of drug dealers, organized crime members, and other common criminals. Simply retaining the "significant purpose" test would allow the slippery slope to occur, making it too easy for secret FISA surveillance to become the norm for law enforcement investigations within the United States.

The missing legislative piece is a requirement within FISA that the surveillance be: (1) important enough; and (2) justifiable on foreign intelligence grounds. Under Title III, the "important enough" element is built into the statute, notably by the requirement that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." n336 The FISA equivalent is considerably looser, with the application requiring only a certification "that such information [*1364] cannot reasonably be obtained by normal investigative techniques." n337 The flaw in this current FISA language is that it allows the slippery slope to occur. A prosecutor investigating a domestic crime can apply for a FISA order if a wiretap will produce information not reasonably available by normal investigative techniques and if the prosecutor can meet the easy standard of "probable cause" that the target is "an agent of a foreign power."

The proposal here, then, is to amend FISA to include a requirement that an application certify that "the information sought is expected to be sufficiently important for foreign intelligence purposes to justify" the initial (and any subsequent) FISA order. In order to keep FISA focused on foreign intelligence surveillance, the usefulness for foreign intelligence purposes would be measured regardless of the usefulness for law enforcement purposes. Three scenarios illustrate the usefulness of the proposed amendment. First, surveillance of a foreign embassy or employees of that embassy would fit within the proposed amendment - the foreign intelligence purposes of watching potential spies in the United States is obvious. Second, the surveillance of suspected Al Qaeda operatives would also meet the test. There are strong foreign intelligence reasons to learn about suspected terrorists. Even if the investigation eventually leads to criminal prosecution, this surveillance is justifiable on foreign intelligence grounds. Third, the use of FISA against drug dealers (potential agents of the Cali cartel) or organized crime mobsters (potential agents of the Russian mafia) would likely be blocked by the FISA amendment. Even if these individuals are considered "agents of a foreign power," it will be difficult to convince the FISC judges that this surveillance is "sufficiently important for foreign intelligence purposes" to justify a FISA order. The amendment proposed here would provide the FISC judges a basis for telling the Justice Department to seek a Title III order if a wiretap is needed.

The proposal here adopts the spirit but not the letter of the "primary purpose" test that existed until the Patriot Act. The spirit of that test, in my view, was to assure that the extraordinary FISA procedures be used only where investigators were seeking to advance foreign intelligence goals. The problem with the letter of the earlier language, however, was that "the wall" sometimes made it too difficult to share information based on the happenstance that investigators might eventually decide that the best way to handle the threat posed by a foreign agent was through prosecution. The proposal here does not prohibit a prosecutor or FBI agent from directing or controlling an investigation, so long as that investigation has the requisite importance for foreign intelligence.

Another virtue of the proposal here is that it can be used when the government seeks to renew or extend a surveillance order. Suppose that an investigation at first seems to be promising in terms of producing foreign intelligence information. The order might result in information that is helpful purely for law enforcement but where there is little prospect of useful foreign intelligence information. In such an instance, any future wiretap order [*1365] would appropriately issue under Title III rather than staying in the FISA system.

D. Improved Procedures for the Foreign Intelligence Surveillance Court System

Experience with the FISA system since 1978, and especially lessons from the FISC and FISCR reported decisions, provides the basis for suggesting reforms for the procedures for handling FISA orders and the use of FISA information in the criminal system.

1. More of an Adversarial System in the FISC

The details of FISC procedures are not publicly available. Department of Justice officials seeking FISA orders present documents to the FISC judges. Members of the Department's OIPR serve certain staff functions for the court. There is no adversarial process, however, and no one is specifically tasked with critiquing the order as it is sought.

Especially as FISA orders are used more aggressively as a means to create evidence for criminal trials, this lack of adversariness becomes more problematic. Congress may thus wish to authorize specifically the creation of a "Team B" or "devil's advocate" role within the FISC process. As a related possibility, the statute might specifically authorize the FISC judges to ask for that sort of representation in a particular case where they believe it would assist the court. The "devil's advocate" would presumably have gone through full security clearance. For instance, the advocate might serve for a period of years and then return to other functions within the Department of Justice. Oversight could be available after the fact to determine the extent to which this innovation has proved helpful.

2. Adversary Counsel in FISCR Appeals

The first case appealed to the FISCR showed a clear gap in existing procedures. Amici were permitted by the court to submit briefs. There was no statutory mechanism, however, that permitted amici or any party opposing the government to participate in an oral argument. Important proceedings at the court of appeals level deserve the possibility of oral argument. Even if some or all of the oral argument of the Department of Justice is closed for security reasons, there can be a separate session involving amici or other parties. In addition, where amici or other parties are represented by persons with security clearances, then the FISCR might decide to include cleared counsel into the entire argument.

3. Possible Certification to the FISC in Criminal Cases

The published FISC opinion provides a picture of that court as developing considerable experience in foreign intelligence matters and considerable awareness of the quality of the evidence being presented before it. It makes sense going forward to take greater advantage of the expertise in the FISC as an institutional way to assure sound decisionmaking on a daily basis.

[*1366] One new role for the FISC could be to review the evidence in cases where a district judge today faces a motion to suppress information derived from a FISA order. It may be difficult for a district court judge, who may never have seen a FISA case before, to assess the extent to which proper procedures were followed in developing evidence in a particular criminal case. One idea for reform would be to permit that district judge, sua sponte or on a motion by defense counsel, to certify the question to the FISC. The FISC could then make a more-informed ruling on the suppression motion, drawing on its experience in the original granting of that particular FISA order and on its experience across the broad range of FISA cases. One advantage of this procedure is that the FISC could compare the representations made to it at the stage of issuing the FISA order with the way that the investigation actually worked out in a criminal prosecu-

tion. If there were misrepresentations in the original FISA application, as happened in the more than seventy-five cases referred to in the FISC opinion, n338 then the FISC judges would be in a position to detect the problem.

4. Create a Statutory Basis for Minimization and Other Rulemaking by the FISC

Article III courts, as part of their inherent authority, play a central role in defining the rules that affect the necessary operations of the courts. Notably, Article III judges play an important role in defining the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, the Federal Rules of Evidence, and the rules applying to contempt of court. n339 It is interesting to consider the extent to which the Article III judges in the FISC should be understood, as a constitutional matter, to have inherent authority to set forth analogous rules for how they implement their judicial role in the FISC. The FISC judges may not wish, as a matter of prudence, to make such a claim. Nonetheless, Congress can consider the extent to which the FISC judges, based on their existing role in the FISA process and their accumulated expertise in foreign intelligence surveillance, should have rulemaking and related supervisory powers over how the FISC operates.

An especially important example of such possible rulemaking would be in the area of minimization. That was the topic of the opinion that the FISC made public - a concern by the judges that the statutory requirement that surveillance be minimized was not being met in practice. The lack of minimization may be a large problem going forward, especially if "the wall" stays down completely and NSLs and section 215 orders permit access to entire databases of records. There is thus a long-run concern that secret FISA orders will be used expansively to intrude into an array of domestic matters. Having enforced minimization procedures is a long-established way to focus [*1367] the surveillance on where it is justified, but not to have open-ended surveillance.

Creation of minimization or other FISC court rules might build on procedures analogous to those used for the federal rules of procedure and evidence. Judges could draft rules subject to comment by the Department of Justice. To the extent possible, the public could comment as well. The rules could actually be implemented after consideration in Congress.

E. Additional Oversight Mechanisms

The reforms proposed above have suggested ways to change the FISC procedures. More rigorous procedures, closer to the criminal model, are appropriate as the use of FISA grows and as it is more aggressively used for explicitly law enforcement purposes. The final set of reforms concerns how to assure long-term oversight of FISA.

1. Reporting on Uses of FISA for Criminal Investigations and Prosecutions

As discussed above, there needs to be greater reporting to Congress and the public of how FISA is used in criminal cases. Without this basic information, it will be difficult for the public and the courts to assess the extent to which the extraordinary foreign intelligence power is being used for "ordinary" criminal investigations. The Title III rules for reporting on the number of prosecutions and convictions are a good model.

2. Disclosure of Legal Theories

The sources and methods used in foreign intelligence investigations are generally sensitive and require secrecy. The names of the targets of the investigation also require secrecy, especially during the period of an active wiretap. The argument for the secrecy of legal theories, however, is much weaker. If the Department of Justice or FBI is taking a novel legal position about the scope of their powers, then the case for congressional and public oversight is especially strong. A statute could require notice to Congress or the public of new legal arguments presented to the FISC. A related, and perhaps more thoughtful, approach would be to allow the FISC to determine whether to release information about legal theories. In that way, the Department of Justice could argue to Article III judges about whether there would be harm to the national security from release of the information.

3. Judiciary Committee Oversight

Historically, the Senate and House Intelligence Committees have been the principal oversight committees for foreign intelligence surveillance. Especially if the "wall" stays down, the Senate and House Judiciary Committees should have a much greater role in oversight. The Judiciary Committees are familiar with the many issues of law enforcement that are outside the scope of the Intelligence Committees.

[*1368]

4. Consider Greater Use of Inspector General Oversight After the Fact

There can be greater after the fact review of the operation of FISA from within the Justice Department or other elements of the intelligence community. A statute might require this sort of oversight, for instance, every three years by the existing Office of the Inspector General or a special office that could be created for foreign intelligence activities. The report of that oversight could be given to the Congressional Intelligence and Judiciary Committees.

5. Consider Providing Notice of FISA Surveillance Significantly After the Fact

For domestic wiretaps, the Fourth Amendment generally requires prompt notice to the target after the wiretap is concluded. For national classified information, even top-secret information, there are declassification procedures with presumptions of release to the public after a stated number of years. n340 Yet for FISA, anomalously, the surveillance remains secret permanently.

Serious consideration should be given to changing the permanent nature of secrecy for at least some FISA surveillance. Procedures can be created that are similar to declassification procedures. For instance, especially in cases that have resulted in criminal prosecution, there might be a presumption of release to the target or the public five years after the surveillance concludes. The presumption of release could be rebutted upon a particularized showing that this particular surveillance should not be made public. The particularized showing, which might be made to the FISC, might be that similar surveillance on the same target (e.g., the same embassy) is continuing or that release of the information would compromise sources and methods. Upon such showing, the FISC might decide to release all of the surveillance, release redacted portions (such as to protect sources and methods), or keep the existence of the surveillance secret.

In making this proposal, I am not wedded to the details of how after the fact surveillance would be released. The growing use of FISA generally, and especially its growing use in law enforcement cases, makes it more important than in 1978 to have effective mechanisms that ensure that the system does not slip into the sort of routine and excessive surveillance that has existed in previous periods. The threat of eventual declassification may serve as an effective check of temptations to overuse FISA powers for political or other improper ends. The reality of eventual declassification may serve the function of the Church Committee hearings, providing evidence that is an essential corrective measure aimed at tendencies of a surveillance system to err on the side of overuse.

Conclusion

As this Article was in the late stages of editing, the world press was filled with pictures and stories about interrogation abuses by members of the U.S. [*1369] military in the Iraqi prison of Abu Ghraib. In October 2003, the top U.S. military official in Iraq signed a classified memorandum that called on intelligence officials to assume control over the "lighting, heating ... food, clothing and shelter" of those being questioned. n341 According to press reports, the subsequent merging of the military intelligence and military police roles was a crucial factor in creating the abuses. n342 Although it is too soon to predict the precise legislative reaction to Abu Ghraib, strict new rules will almost certainly be drafted for military prisons and interrogations.

The tragic events at Abu Ghraib provide vivid lessons for the system of foreign intelligence surveillance law. First, the events of Abu Ghraib demonstrate once again the crucial importance of the rule of law in intelligence and police activities. The history of "The Lawless State" from the time of J. Edgar Hoover now has its counterpart in the lawless activities of interrogators in Iraq. In both instances, abuses were more likely to flourish in settings marked by a lack of clear rules, broad claims of executive discretion, and a philosophy that prevention of future harms justified historically unprecedented measures. n343

Second, Abu Ghraib lets us see the dangers of blurring the boundaries between intelligence and police functions. For the military police at Abu Ghraib, the usual rules for running a prison became subservient to military intelligence goals - an area in which they had not been trained. For the military intelligence personnel at Abu Ghraib, their control over the "lighting, heating ... food, clothing and shelter" of prisoners meant that the usual limits on physical treatment of prisoners did not exist. The result of the blended roles was terrible - the restraints and training that usually guide each group did not apply.

Third, the pragmatic truth is that both national security and civil liberties are fostered by well-drafted procedures for surveillance and interrogation. In [*1370] assessing the effects of the interrogation techniques at Abu Ghraib, any short-term gains for military intelligence were surely minimal compared to the long-term damage. The damage manifested itself in human rights violations and the loss of American prestige in Iraq and the world. It also will almost certainly manifest itself in greater restrictions in the future on the system of military prisons and interrogations. Even from the narrow perspective of increasing the level of military intelligence, the short-run gain from extreme techniques will almost certainly turn out to be less than the long-run loss.

The reform proposals in this Article build on precisely these three lessons: the importance of the rule of law; the risk of blurring intelligence and police functions; and the benefits for both national security and civil liberties from creating effective institutions and rules before a scandal occurs. Concerning the rule of law, this Article has proposed a number of measures that would create a more effective system of checks and balances. For instance, proposals include: greater reporting and oversight; clearer rules of procedure within the FISC and on appeal; abolition of section 215 searches (or at least strict limits) in order to prevent fishing expeditions among U.S. persons; and greater use of Inspector General oversight or declassification of information after the fact.

Concerning the risks of blurring the boundaries between intelligence and police functions, the experience at Abu Ghraib lends new urgency to preventing "the wall" from coming down entirely. With no wall, it will be too easy for the eager prosecutor or FBI agent to minimize the importance of law enforcement procedures in the name of helping intelligence. It will be too easy for the intelligence officer, eager to "connect the dots" in the war on terrorism, to brush aside the stricter rules created by statute and the Constitution that are supposed to apply to U.S. persons. Hence the reform proposal in this Article, to permit the use of the extraordinary FISA powers only upon a certification that "the information sought is expected to be sufficiently important for foreign intelligence purposes" to justify a FISA order. Information used for foreign intelligence would once again be the organizing principle of what would be pursued with FISA authorities. In recognition of the importance of sharing information in pursuit of that goal, bureaucratic requirements of separation would not be required so long as the surveillance was justifiable on foreign intelligence grounds. Greater reporting and oversight of how FISA was used in criminal cases could provide accompanying safeguards.

In terms of the third lesson, how to meet the goals of both national security and civil liberties, the lesson of Abu Ghraib confirms the experience in 1978 from the passage of FISA. The organizing principle in 1978 was that FISA would protect civil liberties, by involving Article III judges in issuance of surveillance orders and providing other statutory safeguards. FISA would also protect national security. By regularizing and legitimizing the ways that foreign intelligence surveillance could proceed, the 1978 Act paved the way for a greater quantity of foreign intelligence orders over time. The experience of Abu Ghraib shows the opposite effect when procedures are badly drafted and have insufficient checks and balances. From a civil liberties perspective, [*1371] the poor procedures contributed to human rights abuses. From a national security perspective, the poor procedures jeopardized the military mission in Iraq and quite possibly will result in a backlash that will impose very strict limits on future interrogation techniques.

My discussions with counterterrorism officials, who preferred to remain anonymous, reveal significant concern about a full removal of "the wall." They have expressed concern about the blurring of intelligence and law enforcement functions: prosecutors and agents have usually not been well-trained in intelligence issues, and their eagerness to use the strong tools of FISA could easily lead to mistakes and over-disclosure of secret sources and methods. Cognizant of the achievements of the 1978 law, they have also expressed concern about the long-run effect of weakening the checks and balances in the FISA system. If FISA gets used excessively or badly in the law enforcement arena, the intelligence professionals are concerned about an eventual backlash. Overuse in the criminal sphere could easily lead to excessive restrictions for the core intelligence activities.

In summary, this Article has presented the first full history and explanation of the development of the system of FISA and the system of foreign intelligence surveillance law. More than thirty years after "The Lawless State" came to light, it is important to remind a new generation about the proven abuses that have occurred in the name of executive discretion and the need to prevent harm. Experience with "The Lawless State" led to creation of the 1978 version of FISA, which both established significant safeguards on national security surveillance and allowed that surveillance to proceed once proper procedures were met. The events of September 11 triggered a new legal era for foreign intelligence surveillance, with major expansion of FISA and the use of NSLs. The rationale for this expansion - that "everything had changed" due to the attacks - is both tempting to believe and subject to serious doubt upon examination.

Where should we go next? This Article has stressed three themes that emerge from the history of FISA and the abuses at Abu Ghraib: the importance of rule of law; the dangers of blending intelligence and police activities; and the benefits for both national security and civil liberties of prescribing effective safeguards in advance. Based on these three principles, the Article has proposed a range of possible legal reforms. Although not all of the proposals are likely to be enacted, it is important to build substantial new checks and balances into the FISA system. The history of previous cycles shows the temptation of surveillance systems to justify an ever-increasing scope of activity, in the hopes that just a little bit more surveillance will catch the terrorists or prevent an attack. Human nature has not fundamentally changed since the Palmer Raids, the McCarthy era, or the revelations of the 1970s. Unless effective institutions are created to limit domestic preventive surveillance, we will likely slip over time into a renewed practice of excessive surveillance. New checks and balances are required to handle new and expanded powers of the executive to keep watch on citizens and keep secret what it learns and how it learns it. The forthcoming sunset of the FISA provisions is a unique historical opportunity to create those checks and balances.

Legal Topics:

For related research and practice materials, see the following legal topics:
Computer & Internet LawCopyright ProtectionCivil Infringement ActionsDefensesGeneral OverviewGovernmentsFederal GovernmentDomestic SecurityGovernmentsFederal GovernmentExecutive Offices

FOOTNOTES:

n1. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. 1801-1811 (2000)).

n2. See infra text accompanying note 36.

n3. Katz v. United States, 389 U.S. 347 (1967); see infra text accompanying notes 21-24.

n4. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

n5. See infra Part IV.A.

n6. See infra text accompanying notes 174-76, 310-22.

n7. See infra text accompanying notes 198-200.

n8. See USA PATRIOT Act 224, 115 Stat. at 295.

n9. In 2003, 1724 surveillance orders were issued under FISA. Letter from William E. Moschella, U.S. Department of Justice, Office of Legislative Affairs, to L. Ralph Mecham, Director, Administrative Office of the United States Courts (Apr. 30, 2004), at http://www.epic.org/privacy/terrorism/fisa/2003 report.pdf. For 2003, 1442 non-FISA wiretap orders were issued under law enforcement authorities. Admin. Office of the U.S. Courts, 2003 Wiretap Report 3 (2004) [hereinafter 2003 Wiretap Report], available at http://www.uscourts.gov/wiretap03/contents.html.

n10. During my service as Chief Counselor for Privacy in the U.S. Office of Management and Budget, I was asked by Chief of Staff John D. Podesta to chair a fifteen-agency White House Working Group on how to update wiretap and other electronic surveillance law for the Internet age. That process resulted in proposed legislation that was introduced to Congress in 2000. See S. 3083, 106th Cong. (2000); see also Press Release, The White House, Assuring Security and Trust in Cyberspace (July 17, 2000), available at http://www.privacy2000.org/presidential/POTUS 7-17-00 fact sheet-on assuring security and trust in cyberspace.htm (announcing legislation proposed by Chief of Staff John D. Podesta in remarks at the National Press Club). For the text of Podesta's remarks, see Press Release, The White House, Remarks by the President's Chief of Staff John D. Podesta on Electronic Privacy to National Press Club (July 18, 2000), available at http://www.privacy2000.org/presidential/POTUS 7-17-00 remarks by podesta on electronic privacy.htm.

n11. See infra text accompanying notes 103-24.

n12. In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611, 615 (Foreign Intel. Surv. Ct. 2002).

n13. See In re Sealed Case (FISCR Decision), 310 F.3d 717 (Foreign Intel. Surv. Ct. Rev. 2002).

n14. See infra Part V.D.

n15. See id.

n16. Olmstead v. United States, 277 U.S. 438 (1928).

n17. See id. at 464-66.

n18. Id. at 478 (Brandeis, J., dissenting).

n19. For the history, see Orin S. Kerr, Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't, 97 Nw. U. L. Rev. 607, 630 (2003).

n20. For a detailed study of the historical weaknesses of protections at the state level, see Samuel Dash et al., The Eavesdroppers (De Capo Press 1971) (1959); see also Charles H. Kennedy & Peter P. Swire, State Wiretaps and Electronic Surveillance After September 11, 54 Hastings L.J. 971, 977 (2003) (analyzing the history and current practice of state wiretap laws); id. at app. A (fifty-state survey of state laws on wiretaps, stored records, pen registers, and trap and trace orders); id. at app. B (survey of state wiretap law changes in the first nine months after the events of September 11).

n21. Katz v. United States, 389 U.S. 347 (1967).

n22. Id. at 353.

n23. The "reasonable expectation of privacy" test was announced by Justice Harlan in Katz. Id. at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"). This doctrinal test has since been adopted. See, e.g., Kyllo v. United States, 533 U.S. 27, 33 (2001); California v. Ciraolo, 476 U.S. 207, 211 (1986).

Professor Orin Kerr has recently argued that the federal courts have only rarely departed from traditional, property-based understandings of what is protected by the Fourth Amendment, and thus have used the "reasonable expectation of privacy test" much less than most observers have realized. See Orin Kerr, The Fourth Amendment in New Technologies: Constitutional Myths and the Case for Restraint, 102 Mich. L. Rev. (forthcoming 2004). For my response to Professor Kerr, see Peter P. Swire, Katz is Dead. Long Live Katz, 102 Mich. L. Rev. (forthcoming 2004).

n24. Katz, 389 U.S. at 358 n.23.

n25. Berger v. New York, 388 U.S. 41, 54-64 (1967).

n26. See id.

n27. See infra text accompanying notes 108-12.

n28. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified at 18 U.S.C. 2510-2521 (2000)).

n29. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

n30. Electronic communications lack three of the protections that apply to wire and oral communications: the requirement of high-level Department of Justice approval before conducting the surveillance, 18 U.S.C. 2516(1) (2000); restriction to a list of serious offenses, id.; and, most significantly, no application of the relatively strict rules for suppressing evidence obtained in violation of the applicable rules, id. 2515. In 2000, as part of the process in which I was involved, the Clinton Administration proposed applying these three protections to electronic communications. See supra note 10. This proposal has not been enacted.

n31. See Peter P. Swire, Administration Wiretap Proposal Hits the Right Issues But Goes Too Far, Brookings Terrorism Project Website (Oct. 3, 2001), available at http://www.brookings.edu/dybdocroot/views/articles/fellows/2001 Swire.htm. Professor Kerr has claimed that the Patriot Act actually increased privacy protections in the area of domestic electronic surveillance. Kerr, supra note 19, at 608. I have discussed these issues at length with Professor Kerr, and he moderated his claims substantially from the early working paper to final publication. In essence, Professor Kerr finds an increase in privacy protection where the Patriot Act codified the permissibility of surveillance in situations where arguably law enforcement was previously free to act without statutory or constitutional restraint. Id. My critique of that approach is fourfold. First, there quite possibly are or should be constitutional limits on some of the surveillance that the Patriot Act apparently authorizes. Second, the Act sets the statutory standards so low in Professor Kerr's examples that any privacy protections are minimal at best. Third, if the Department of Justice had publicly claimed the even broader surveillance powers that Professor Kerr asserts it might possess, then there quite possibly would have been a political reaction from Congress to limit those broader surveillance powers. Fourth, any modest privacy gains that Professor Kerr might identify are outweighed by other aspects of the Act that reduce privacy in the electronic surveillance area, especially in the area of foreign intelligence surveillance discussed in this Article.

n32. See, e.g., Atossa M. Alavi, The Government Against Two: Ethel and Julis Rosenberg's Trial, 53 Case W. Res. L. Rev. 1057, 1059 (2003) (identifying Klaus Fuchs as the supplier of nuclear technology to the Soviets); Joseph Finder, The Spy Who Sold Out, N.Y. Times, July 2, 1995, 7 (Late Edition), at 5 (criticizing Aldrich Ames for selling double agent identities).

n33. U.S. Const. art. II, 3.

n34. United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304 (1936).

n35. Id. at 320.

n36. See Alison A. Bradley, Comment, Extremism in the Defense of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT ACT, 77 Tul. L. Rev. 465, 468 (2002) (describing limited nature of national security wiretaps authorized by President Roosevelt).

n37. Katz v. United States, 389 U.S. 347, 358 n.23 (1967).

n38. N.Y. Times Co. v. United States, 403 U.S. 713, 727 (1971) (Stewart, J., concurring); see Stephen Dycus et al., National Security Law ch. 4, at 60-91 (3d ed. 2002) (analyzing growth of executive power in national security realm).

n39. United States v. U.S. Dist. Court (Keith), 407 U.S. 297 (1972).

n40. Id.

n41. Id. at 299.

n42. Id. at 299-300.

n43. Id. at 300 n.2.

n44. See id. at 301.

n45. Id.

n46. Id. at 324 (noting that "Mr. Justice Rehnquist took no part in the consideration or decision of this case").

n47. Id. at 302 (quoting 18 U.S.C. 2511(3)).

n48. Id. at 308. Later, the Court reiterated the point: "We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents." Id. at 321-22 (citation omitted).

n49. Id. at 309 (quoting Katz v. United States, 389 U.S. 347, 358 n.23).

n50. Id. at 310 (quoting U.S. Const. art. II, 1).

n51. Id. at 319-21.

n52. Id. at 320.

n53. Id. at 322.

n54. Id.

n55. Id.

n56. Id. at 323.

n57. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. 1801-1811 (2000)).

n58. Morton H. Halperin et al., The Lawless State: The Crimes of the U.S. Intelligence Agencies (1976).

n59. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, 94th Cong., Final Report on Intelligence Activities and the Rights of Americans, Book II, I (1976) [hereinafter Church Final Rep. IIa] (internal citations omitted), available at http://www.icdc.com/paulwolf/cointelpro/churchfinalreportIIa.htm.

n60. Id. (footnotes omitted).

n61. E.g., Halperin et al., supra note 58, at 3 (estimating the number of surveillance crimes committed); id. at 93 (describing surveillance violations by the FBI).

n62. Church Final Rep. IIa, supra note 59.

n63. Id.

n64. Id.

n65. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, 94th Cong., Final Report on Intelligence Activities and the Rights of Americans, Book II, II (1976) [hereinafter Church Final Rep. IIb] (internal citations omitted), available at http://www.icdc.com/paulwolf/cointelpro/churchfinalreportIIb.htm.

n66. Id.

n67. Church Final Rep. IIa, supra note 59.

n68. Id.

n69. Id.

n70. "The FBI practice of supplying political information to the White House ... under the administrations of President Lyndon Johnson and Richard Nixon ... grew to unprecedented dimensions." Church Final Rep. IIb, supra note 65.

n71. Id. Examining evidence of use of intelligence information against political opponents, the committee concluded: "A domestic intelligence program without clearly defined boundaries almost invited such action." Id.

n72. Halperin et al., supra note 58, at 124.

n73. Church Final Rep. IIa, supra note 59.

n74. Id.

n75. See Halperin et al., supra note 58, at 86. The Church Committee reported on the breadth of the FBI's infiltration of the black community: "In 1970, the FBI used its 'established informants' to determine the 'background, aims and purposes, leaders and Key Activists' in every black student group in the country, 'regardless of [the group's] past or present involvement in disorders.'" Church Final Rep. IIb, supra note 65.

n76. Church Final Rep. IIa, supra note 59.

n77. Id.

n78. Id.

n79. Id.

n80. Id.

n81. Church Final Rep. IIb, supra note 65; see also Richard G. Powers, Secrecy and Power: The Life of J. Edgar Hoover 429 (1987).

n82. Church Final Rep. IIa, supra note 59.

n83. Id.

n84. Id.

n85. Hearing on Foreign Intelligence Surveillance Act, 95th Cong. 147-48 (1979) (statement of Jerry Berman).

n86. The current definition is codified at 50 U.S.C. 1801(a) (2000).

n87. 50 U.S.C. 1801(a)(1).

n88. Id. 1801(a)(2), (5).

n89. Id. 1801(a)(4).

n90. See id. 1801(b).

n91. Id. 1801(b)(2)(C).

n92. See id. 1801(c). The term "international terrorism" was defined in full as:

Activities that - (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended - (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Id.

n93. Id. 1801(i).

n94. Id.

n95. Id. 1801(b)(1)(A).

n96. Id. 1801(b)(2)(A).

n97. United States v. U.S. Dist. Court (Keith), 407 U.S. 297 (1972).

n98. Id. at 308, 321-22.

n99. The 1978 law created the split by providing, in terms still effective today, that Title III and FISA "shall be the exclusive means by which electronic surveillance ... and the interception of domestic wire and oral communications may be conducted." 18 U.S.C. 2511(2)(f) (2000).

n100. 50 U.S.C. 1803.

n101. Id. 1805(a)(3)(A).

n102. 18 U.S.C. 2518(3)(a) (2000).

n103. Compare 50 U.S.C. 1805(a)(2) (approval by the Attorney General for FISA applications), with 18 U.S.C. 2518(11)(b)(i) (approval also permitted for domestic surveillance by the Deputy Attorney General, the Associate Attorney General, or an acting or confirmed Assistant Attorney General). The officers other than the Attorney General were added in 1984. Act of Oct. 12, 1984, Pub. L. No. 98-473, 98 Stat. 1837 (codified at 18 U.S.C. 1203(a) (2000)).

n104. Compare 50 U.S.C. 1805(a)(4) (FISA applications), with 18 U.S.C. 2518(5) (Title III applications).

n105. Compare 50 U.S.C. 1805(e) (FISA applications), with 18 U.S.C. 2518(5) (Title III applications).

n106. Compare 50 U.S.C. 1805(c)(1) (FISA applications), with 18 U.S.C. 2518(4) (Title III applications).

n107. FISA originally required judicial approval of an emergency order within twenty-four hours, but this was extended to seventy-two hours in 2001. Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, 314(a)(2)(B), 115 Stat. 1394, 1402 (2001) (codified at 50 U.S.C.A. 1805(f) (West 2003)). Title III emergency orders must be approved by a judge within forty-eight hours. 18 U.S.C. 2518(7).

n108. "Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception ... ." 18 U.S.C. 2518(3) (emphasis added).

n109. 50 U.S.C. 1805(a).

n110. Title III requires that a wiretap or other electronic surveillance be a last resort, available only when "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. 2518(3)(C). Under FISA, the application must simply certify "that such information cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. 1804(7)(C).

n111. Title III requires notice "within a reasonable time but not later than ninety days" after surveillance expires. 18 U.S.C. 2518(8)(d). Notice is given to the persons named in the order and others at the judge's discretion. Id. An inventory is provided concerning the dates and scope of surveillance. Id. In the judge's discretion, the person or counsel may inspect such intercepted communications, applications, and orders as the judge determines to be in the interest of justice. Id. The judge may also, on a showing of good cause, postpone notice. Id.

n112. These procedures are set forth in 50 U.S.C. 1806. In ruling on a suppression motion, the judge "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." Id. 1806(f). If the court determines that the surveillance was conducted lawfully, "it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." Id. 1806(g).

n113. See 50 U.S.C. 1802(a)(1)(A)(i).

n114. See id. 1808(a). In the initial years after passage of FISA, the Intelligence Committees were additionally required to report to the full House and Senate about the operation of the statute. Id. 1808(b).

n115. Id. 1807.

n116. See 18 U.S.C. 2529 (reports on Title III wiretaps); see also 18 U.S.C. 3126 (2000) (reports on pen register and trap and trace orders).

n117. See infra Part IV.C.

n118. See Electronic Privacy Information Center, Foreign Intelligence Surveillance Act Orders 1979-2002, http://www.epic.org/privacy/wiretap/stats/fisa stats.html (last updated May 6, 2004) (giving annual statistics of FISA orders). The 2003 FISA Report stated that three additional orders were denied in 2003. Letter from William E. Moschella, U.S. Department of Justice, Office of Legislative Affairs, to L. Ralph Mecham, Director, Administrative Office of the United States Courts (Apr. 30, 2004), at http://www.epic.org/privacy/terrorism/fisa/2003 report.pdf. At the time of this writing, no further information was available to the public about the three denials.

n119. 50 U.S.C. 1805(a)(2).

n120. E.g., Jim McGee & Brian Duffy, Main Justice 309 (1996).

n121. See, e.g., Jeff Nesmith et al., Subtle Forces Swirl Just Beneath Siege Inquires: The Tug of Personality Conflict in Washington Alters Flow of Waco Controversy, Austin Am.-Statesman, Sept. 19, 1999, at A1 (discussing "tension" between the Department of Justice and the FBI, and between Attorney General Reno and FBI Director Freeh).

n122. 50 U.S.C. 1805(a)(3)(A).

n123. See Church Final Rep. IIa, supra note 59 (noting that between 1960 and 1974, "subversion" alone was used to justify more than 500,000 investigations, with apparently no prosecutions for the actual crimes).

n124. 50 U.S.C. 1804(7). This language was changed in 2001 to say that "a significant purpose of the investigation is to obtain foreign intelligence information." Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 218, 115 Stat. 272, 291 (codified at 50 U.S.C.A. 1804(7) (West 2003)); see also infra Part IV.A.1.

n125. See generally Arthur M. Schlesinger, The Imperial Presidency (1973).

n126. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, 1896 (codified at 5 U.S.C. 552a (2000)).

n127. Freedom of Information Act, Pub. L. No. 93-502, 4, 88 Stat. 1561, 1564 (1974) (amending 5 U.S.C. 552).

n128. Government in the Sunshine Act, Pub. L. No. 94-409, 90 Stat. 1241 (1976) (codified as amended at 5 U.S.C. 552b).

n129. See generally The Reporters' Committee for Freedom of the Press, Tapping Officials' Secrets, http://www.rcfp.org/tapping (last visited July 29, 2004) (collecting state open meeting laws).

n130. See Carl Bernstein & Bob Woodward, All the President's Men (1974); Carl Bernstein & Bob Woodward, The Final Days (1977).

n131. Attorney General, U.S. Dep't of Justice, Domestic Security Investigations (1976). For subsequent versions of these guidelines, see Electronic Privacy Information Center, The Attorney General's Guidelines, http://www.epic.org/privacy/fbi (last updated Mar. 17, 2003) [hereinafter Attorney General's Guidelines] (including comprehensive links to subsequent domestic surveillance guidelines and related materials).

n132. Attorney General, U.S. Dep't of Justice, Domestic Security Investigations (1976).

n133. Id.

n134. McGee & Duffy, supra note 120, at 311.

n135. For instance, shortly after I left the government I had a lengthy conversation with a senior FBI lawyer who had watched the changes over previous decades. He frankly admitted that the Bureau had not worried much about breaking the law before the mid-1970s. He said that the painful revelations and the bad effects on the careers of those caught up in those revelations had led to a profound change in the organization's culture. The Bureau, by early 2001, had developed a culture of compliance. These statements tracked the views of a very knowledgeable insider with whom I worked in government. He agreed that the FBI had generally learned to follow the rules since the 1970s. He also believed that they often had very aggressive interpretations of the rules, and they stayed within the limits of their interpretation.

This shift to a culture of compliance has some important implications. First, these observations on the Bureau's behavior underscore the importance of rules such as the Attorney General Guidelines. If an agent complies with a set of defined rules, then the content of those rules matters. Second, the lessons from the 1970s deeply impressed a generation of FBI employees with the risks of excessive surveillance and intrusion into First Amendment activities. With the passage of time, fewer veterans of that experience will remain in the Bureau, and the impact of those lessons will be less, potentially raising the risk of renewed abuses.

n136. McGee & Duffy, supra note 120, at 314.

n137. For an admiring portrait of Mary Lawton and her role in shaping foreign intelligence law until her death in 1993, see the chapter entitled "Mary's Law" in McGee & Duffy, supra note 120, at 303-19.

n138. Id. at 318.

n139. See supra note 124 and accompanying text.

n140. Id.

n141. The Senate Report on FISA stated, "'Contrary to the premises which underlie the provision of Title III of the Omnibus Crime Control Act of 1968 ... it is contemplated that few electronic surveillances conducted pursuant to [FISA] will result in criminal prosecution.'" McGee & Duffy, supra note 120, at 326-27 (quoting members of the Senate Select Committee on Intelligence, 1978 Report).

n142. Memorandum from Janet Reno, Attorney General, to Assistant Attorney General, Criminal Division, FBI Director, Counsel for Intelligence Policy, and United States Attorneys (July 19, 1995), http://www.fas.org/irp/agency/doj/fisa/1995procs.html. For a description of the genesis and contents of the 1995 guidelines, see McGee & Duffy, supra note 120, at 327-43.

n143. Memorandum from Janet Reno, supra note 142.

n144. Id. A.2.

n145. Id. A.7.

n146. E.g., United States v. Duggan, 743 F.2d 59, 71 (2d Cir. 1984) (no violation of Fourth Amendment or the separation of powers); United States v. Belfield, 692 F.2d 141, 149 (D.C. Cir. 1982) (no violation of Fifth or Sixth Amendment rights); United States v. Falvey, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982) (no violation of First Amendment rights).

n147. Duggan, 743 F.2d at 77-78. For a discussion of other cases that also used the "primary purpose" test, see infra note 217 and accompanying text.

n148. See Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, 807, 108 Stat. 3444, 3444-45 (1994) (codified as amended at 50 U.S.C. 1821-1829 (2000)).

n149. See Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, 601(2), 112 Stat. 2396, 2405-10 (1998) (codified at 50 U.S.C. 1841-1846 (2000)).

n150. Id. 602, 112 Stat. at 2411-12 (codified at 50 U.S.C. 1861-1862 (2000)) (permitting access held by common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities).

n151. Electronic Privacy Information Center, supra note 118.

n152. Id.

n153. Id.; Letter from William E. Moschella, supra note 118.

n154. 2003 Wiretap Report, supra note 9, at 3.

n155. Id. For discussion of the relative lack of institutional safeguards on wiretaps conducted at the state level, see Kennedy & Swire, supra note 20, at 977-83.

n156. The greatest concerns were expressed about FBI surveillance of the Committee in Solidarity with the People of El Salvador in the 1980s. Attorney General's Guidelines, supra note 131.

n157. For instance, FISA wiretaps and search authorizations increased from 484 in 1992 to 839 in 1996 (after the Oklahoma City and first World Trade Center incidents), while federal Title III wiretaps increased more slowly, from 340 in 1992 to 581 in 1996. See Electronic Privacy Information Center, supra note 118; Electronic Privacy Information Center, Title III Electronic Surveillance 1968-2002, available at http://www.epic.org/privacy/wiretap/stats/wiretap stats.html (last visited July 5, 2004) (listing Title III statistics).

n158. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

n159. Id. For an illuminating and detailed account of the passage of the Act, see Beryl A. Howell, Seven Weeks: The Making of the USA PATRIOT Act, 72 Geo. Wash. L. Rev. 1145 (2004).

n160. 50 U.S.C. 1804(7) (2000).

n161. See cases cited supra notes 146-47 and accompanying text.

n162. Section 153 of the administration's original proposal would have changed "the purpose" to "a purpose." Center for Democracy & Technology, Testimony of Jerry Berman before the Senate Select Comm. on Intelligence on Legislative Measures to Improve America's Counter-Terrorism Programs (Sept. 24, 2001), available at http://www.cdt.org/testimony/010924berman.shtml.

n163. USA PATRIOT Act 218, 115 Stat. at 291.

n164. Section 203 of the Patriot Act made it significantly easier for grand jury information to be shared for foreign intelligence and counterintelligence purposes. Id. 203(a), 115 Stat. at 278-81. It also provided:

Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence ... information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.

Id. 203 (d), 115 Stat. at 281.

n165. Id. 215, 115 Stat. at 287-88.

n166. See Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, 602, 112 Stat. 2396, 2411-12 (1998) (codified at 50 U.S.C. 1861-1862 (2000)) (permitting access held by common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities).

n167. USA PATRIOT Act 218, 115 Stat. at 287.

n168. 50 U.S.C.A. 1861(b)(2)(B) (West 1999) (current version at 50 U.S.C.A. 1861(b)(2) (West 2003)).

n169. 50 U.S.C.A. 1861(b)(2) (West 2003).

n170. See id.

n171. See id.

n172. An analogous point was made by Justice Stevens concerning the expansion of searches in the law enforcement setting:

Just as the witnesses who participate in an investigation or a trial far outnumber the defendants, the persons who possess evidence that may help to identify an offender, or explain an aspect of a criminal transaction, far outnumber those who have custody of weapons or plunder. Countless law-abiding citizens - doctors, lawyers, merchants, customers, bystanders - may have documents in their possession that relate to an ongoing criminal investigation.

Zurcher v. Stanford Daily, 436 U.S. 547, 579 (1978) (Stevens, J., dissenting).

n173. See 50 U.S.C.A. 1861.

n174. For my discussion of the expanded power of the government to get records in the area of criminal investigations, see Swire, supra note 23.

n175. See infra notes 325-26 and accompanying text (discussing gag rule in section 215).

n176. 50 U.S.C.A. 1861(d).

n177. NSLs are permitted under the Electronic Communications Privacy Act, 18 U.S.C. 2709 (2000), for telephone and electronic communications records; the Right to Financial Privacy Act of 1978, 12 U.S.C. 3414(a)(5)(A) (2000), for financial records; and the Fair Credit Reporting Act, 15 U.S.C. 1681u (2000), for credit records.

n178. 18 U.S.C. 2709(b)(1)(B).

n179. 18 U.S.C.A. 2709 (b)(1) (West 2003). As a modest safeguard, the Patriot Act included the requirement that "an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." Id.

n180. 18 U.S.C.A. 2709(b)(2)(A) (West 1999).

n181. 18 U.S.C.A. 2709(b)(1) (West 2003).

n182. 18 U.S.C.A. 2709(b) (West 1999).

n183. 18 U.S.C.A. 2709(b) (West 2003).

n184. The individual may discover the use of the NSL if a criminal prosecution is later brought.

n185. Dan Eggen & Robert O'Harrow, Jr., U.S. Steps up Secret Surveillance, Wash. Post, Mar. 23, 2003, at A1 (reporting on congressional testimony).

n186. Eric Lichtblau & James Risen, Broad Domestic Role Asked for C.I.A. and the Pentagon, N.Y. Times, May 2, 2003, at A21.

n187. 50 U.S.C. 1842(c)(3) (2000).

n188. 50 U.S.C.A. 1842(c)(2) (West 2003). For discussion of the domestic standard for pen register and trap and trace orders, see Peter P. Swire, Administration Wiretap Proposal Hits the Right Issues But Goes Too Far http://www.brookings.edu/dybdocroot/views/articles/fellows/2001 swire.htm (Oct. 3, 2001).

n189. See 18 U.S.C. 2518(11)-(12) (2000).

n190. 50 U.S.C.A. 1805(c)(2)(B) (West 2003). For a critique of post-Patriot Act proposals by the Department of Justice to expand roving wiretaps further, see Center for Democracy and Technology, DOJ Proposes Further Surveillance Expansion Changes to Intelligence Authorization Would Again Increase FISA Eavesdropping, http://www.cdt.org/security/011130cdt.shtml (Nov. 30, 2001).

n191. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 224, 115 Stat. 272, 295. The expanded NSL authority in section 505 of the Patriot Act does not sunset. See id.

n192. In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611, 619 (Foreign Intel. Surv. Ct. 2002).

n193. See In re Sealed Case (FISCR Decision), 310 F.3d 717, 729 (Foreign Intel. Surv. Ct. Rev. 2002).

n194. Id.

n195. Id.

n196. Id.

n197. See supra notes 131-32 and accompanying text.

n198. Attorney General John Ashcroft, Remarks on Attorney General Guidelines (May 30, 2002), http://www.fas.org/irp/news/2002/05/ag053002.html.

n199. Id.

n200. Jerry Berman & James X. Dempsey, CDT's Guide to the FBI Guidelines: Impact on Civil Liberties and Security - The Need for Congressional Oversight (June 26, 2002), http://www.cdt.org/wiretap/020626guidelines.shtml. The concerns about infringement of the First Amendment that were so prominent in the Levi Guidelines were given much less weight in the new guidelines: "The law enforcement activities authorized by this Part do not include maintaining files on individuals solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States." U.S. Dep't of Justice, The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations 23 (2002) (emphasis added), available at http://www.usdoj.gov/olp/generalcrimes2.pdf. This language, which tracks the FISA restriction on surveillance "solely" on the basis of First Amendment activities, gives wide permission for surveillance that affects First Amendment activities. See id.

n201. See cases cited supra notes 192-93.

n202. The USA Patriot Act in Practice: Shedding Light on the FISA Process: Hearing Before the Committee on the Judicary, 107th Cong. (2002) (statement of Sen. Patrick Leahy, Chairman, Senate Comm. on Judiciary), http://www.fas.org/irp/congress/2002 hr/091002leahy.html.

n203. In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611, 622, 625 (Foreign Intel. Surv. Ct. 2002).

n204. See id. at 621; see also 50 U.S.C. 1801(h)(1), 1821(4)(A) (2000).

n205. 50 U.S.C. 1801(h)(1), 1821(4)(A).

n206. FISC Decision, 218 F. Supp. 2d at 625.

n207. Id. at 620.

n208. Id. at 620-21. For instance, one certification by the FBI Director stated erroneously that the target of the FISA application was not under criminal investigation. After a meeting by the judges and the Department of Justice, one FBI agent was barred from appearing before the FISC as a FISA affiant and an investigation was opened by the Justice Department's Office of Professional Responsibility. See id.

n209. Id. at 621.

n210. The court wrote that the 1995 guidelines implementing the "wall" were "an integral part of the minimization process." Id. at 619.

n211. Id. at 623 (quotation omitted).

n212. See In re Sealed Case (FISCR Decision), 310 F.3d 717, 746 (Foreign Intel. Surv. Ct. Rev. 2002).

n213. Id. at 725-35.

n214. Id. at 735.

n215. Id. at 721.

n216. Id. at 723.

n217. Id. at 725-27 (discussing United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980) (concerning surveillance done before enactment of FISA)).

n218. Id. at 727.

n219. See In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611, 625 (Foreign Intel. Surv. Ct. 2002).

n220. See id.

n221. See id.

n222. FISCR Decision, 310 F.3d at 725 (quoting H.R. Rep. No. 95-1283, at 36 (1978)).

n223. Id.

n224. Id. at 732. The court quotes Senator Leahy, who considered the change "'very problematic,'" as saying that it "'would make it easier for the FBI to use a FISA wiretap to obtain information where the Government's most important motivation for the wiretap is for use in a criminal prosecution.'" Id. at 733 (quoting 147 Cong. Rec. S10,593 (daily ed. Oct. 11, 2001) (statement of Sen. Leahy)).

n225. Id. at 735.

n226. Id. The court noted that "if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct - even foreign intelligence crimes - to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied." Id. (emphasis added).

n227. See supra notes 159-64 and accompanying text (discussing amendment debate).

n228. The briefs are available at http://www.epic.org/privacy/terrorism/fisa/FISCR amicus brief.pdf. The ACLU joined with the Center for Democracy and Technology, the Center for National Security Studies, the Electronic Privacy Information Center, and the Electronic Frontier Foundation. The Court permitted the amici to file briefs but allowed only the Department of Justice to appear at oral argument. See id.

n229. See FISCR Decision, 310 F.3d at 744.

n230. See id. at 744-45.

n231. See id. at 741-42.

n232. Id. at 741.

n233. In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611, 625 (Foreign Intel. Surv. Ct. 2002).

n234. 18 U.S.C. 2510 (2000).

n235. See id. 2518(8); supra note 111.

n236. E.g., Silas J. Wasserstrom & Louis Michael Seidman, The Fourth Amendment as Constitutional Theory, 77 Geo. L.J. 19, 66 (1988).

n237. 50 U.S.C.A. 1806 (West 2001); see supra notes 111-12 and accompanying text.

n238. See 50 U.S.C.A. 1806.

n239. For an extended and effective explanation of the usefulness of comparative institutional analysis, see Neil K. Komesar, Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy (1995).

n240. See supra notes 16-27 and accompanying text.

n241. See supra notes 111-12 and accompanying text.

n242. See United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 324 (1972).

n243. Id. at 321-22.

n244. See supra notes 97-99 and accompanying text.

n245. The term "constitutional moment" is associated with Bruce Ackerman. See 1 Bruce Ackerman, We the People: Foundations 266-94 (1991). My use of the term here is not intended to take a definite position on the complex scholarly disputes about the details of Professor Ackerman's theory or of the history that surrounded the periods that Professor Ackerman chooses for special study. See, e.g., Michael J. Klarman, Constitutional Fact/Constitutional Fiction: A Critique of Bruce Ackerman's Theory of Constitutional Moments, 44 Stan. L. Rev. 759 (1992) (critiquing Ackerman position). Instead, the term usefully captures the unique historical moment of Watergate and the constitutional-style reforms that led to checks on the Imperial Presidency in measures such as greater openness of government and reduced secret surveillance.

n246. See supra notes 61-84 and accompanying text.

n247. See generally Hearings Before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence, 95th Cong. 3 (1978) (balancing the efficiency benefits of allowing more surveillance rights against the benefits of privacy) (statement of Robert McClory); Hearing Before the Subcomm. on the Rights of Americans, 95th Cong. (1977) (considering the historical power to use surveillance inherent to the President and the Fourth Amendment rights that might outweigh it); Surveillance Technology: Policy and Implications: An Analysis and Compendium of Materials, 95th Cong. 378 (1977) (considering the benefits of other agencies having access to methods of surveillance).

n248. For a rhetorical attack on the view that "everything has changed," see Magniloquence Against War!, Everything Has Changed, or Has It?, http://irregulartimes.com/everything.html (last visited July 29, 2004). For a recent set of academic essays on the subject, see September 11 in History: A Watershed Moment? (Mary L. Dudziak, ed., 2004). The historian and legal scholar Mary Dudziak stated:

The assumption that September 11 had been a moment of change was again ubiquitous. Yet, in an unscientific poll taken by the Web site for historians History News Network, 67 percent of respondents answered "no" to the question, "On balance, would you say that 9-11 changed America in a decisive way?" Only 28 percent thought that it had.

Mary L. Dudziak, Afterward: Remembering September 11, in September 11 in History: A Watershed Moment? supra, at 212. This Article agrees with the majority of historians by putting the attacks of September 11 into historical context, both by giving the history of previous government abuse of surveillance powers, supra notes 59-84 and accompanying text, and by comparing the threat posed by terrorism after September 11 with the equivalent or greater threats that faced the United States in previous periods, infra notes 256-70 and accompanying text.

n249. President George W. Bush, Address to a Joint Session of Congress (Sept. 20, 2001), http://www.everythingcomputers.com/presbushspeech.htm.

n250. In developing the argument for the magnitude of the threat and the other arguments, I am attempting to present the arguments for greater surveillance in a coherent way, and the statements in the text do not necessarily reflect my own judgment about the facts.

n251. Six Yemeni-Americans living in Lackawanna, New York pled guilty in 2003 to providing material support to a terrorist organization. See Man Who Trained with Qaeda Gets 10-Year Sentence, N.Y. Times, Dec. 4, 2003, at A37. The six reportedly received weapons training in Afghanistan in the spring of 2001 and heard

Osama bin Laden speak in person. Id. Prosecutors suggested that the six might have constituted a sleeper cell, available for possible future terrorist attacks in the United States, but the six denied that accusation. Id.

n252. FBI Director Mueller said in 2003 that the prevention of terror attacks was the top priority of the agency. David Johnson, 9/11 Congressional Report Faults F.B.I.-C.I.A. Lapses, N.Y. Times, July 23, 2003, at A12.

n253. See, e.g., Editorial, Tearing Down Intelligence Walls, Chi. Trib., Nov. 9, 2003, 2, at 8.

n254. On funding, for instance, "from fiscal years 1995 to 1998, the FBI more than doubled its allocation of resources for combating terrorism." GAO, Combating Terrorism: FBI's Use of Federal Funds for Counterterrorism-Related Activities (FYs 1995-1998) 2 (1998), http://www.gao.gov/archive/1999/gg99007.pdf.; see also Barton Gellman, Struggles Inside the Government Defined Campaign, Wash. Post, Dec. 20, 2001, at A1 (examining funding increases and other Clinton Administration antiterrorism actions, concluding, "by any measure available, Clinton left office having given greater priority to terrorism than any president before him"). For the rise in the number of FISA orders, see supra notes 152-55 and accompanying text.

n255. See James B. Simpson, Simpson's Contemporary Quotations (1988), http://www.bartleby.com/63/38/4638.html.

n256. See generally Nancy Murray & Sarah Wunsch, Civil Liberties in Times of Crisis: Lessons from History, 87 Mass. L. Rev. 72 (2002).

n257. See id.

n258. See id.

n259. United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 311 n.12 (1972). The Supreme Court noted that this statistic was subject to dispute and stated that the "precise level of this activity ... is not relevant to the disposition of this case." Id.

n260. For an insightful history of the McCarthy period, see Mary L. Dudziak, Cold War Civil Rights (2000).

n261. Jonathan Schell, The Fate of the Earth 6 (1982).

n262. For a somewhat similar analysis, see Jonathan Rauch, Osama Bin Laden, Meet Your Closest Kin: Karl Marx, Nat'l J., July 13, 2002, http://reason.com/rauch/071302.shtml ("In many respects, militant Islam is weaker than Marxism was in its heyday.").

n263. For a detailed historical examination of Alger Hiss, see G. Edward White, Alger Hiss's Campaign for Vindication, 83 B.U. L. Rev. 1 (2003).

n264. See Powers, supra note 81, at 375-80.

n265. Id. at 427.

n266. The most publicized of such action was likely the thwarting of the "millennium attacks" by associates of Osama bin Laden. Michael Isikoff et al., Al Qaeda's Summer Plans, Newsweek, June 2, 2003, at 24. For a detailed recent account, see Richard A. Clarke, Against All Enemies 211-15 (2004).

n267. See In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611, 620-621 (Foreign Intel. Surv. Ct. 2002).

n268. Hearing of the Senate Judiciary Comm: Oversight on Counterterrorism Efforts by the FBI, 107th Cong. 78 (2002) (statement of Coleen Rowley).

n269. Hearing of the National Comm. on Terrorist Attacks upon the United States, Panel IV: Governmental Organization and Domestic Intelligence, 108th Cong. 92 (2003) (statement of John MacGaffin).

n270. House Select Homeland Sec. Comm., 9/11 Intelligence Report, 108th Cong. (2003) (statement of Eleanor Hill).

n271. See 50 U.S.C. 1805(f) (2000). A similar emergency provision exists for Title III wiretaps. 18 U.S.C. 2518(7) (2000).

n272. 50 U.S.C. 1805(f).

n273. Id. The time for an emergency order was extended from twenty-four to seventy-two hours in the Patriot Act. Uniting and Strengthening American by Providing the Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 314(a)(2)(B), 115 Stat. 272, 307 (codified at 50 U.S.C.A. 1805(f) (West 2003)).

n274. Eggen & O'Harrow, supra note 185 (reporting on congressional testimony).

n275. For those of us in this electronic age who rarely work with physical machines, a "ratchet" is a device that acts in one direction only, such as where pressure is increased over time.

n276. For an overview of this complexity, see Kerr, supra note 19.

n277. See supra notes 158-91 and accompanying text (describing statutory expansions in the 1990s). In the Patriot Act, an example of a ratcheting up of surveillance power was the changed treatment of voice mail. Under Title III, stored voice recordings were considered "wire" communications, just like actual telephone calls. Under the Patriot Act, however, stored voice recordings were shifted to the category of "stored records," subject to easier access by law enforcement. Computer Crime and Intellectual Prop. Section, U.S. Dept. of Justice, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last updated Nov. 5, 2001).

n278. One especially clear example of this form of policy argument came in the so-called "Patriot II" proposal by the Bush administration that was leaked in early 2003. See Charles Lewis & Adam Mayle, Justice Dept. Drafts Sweeping Expansion of Anti-Terrorism Act (Feb. 7, 2003), http://publicintegrity.org/dtaweb/report.asp?ReportID=502&L1=10&L2=10&L3=0&L4= 0&L5=0. The proposal, when leaked, was advanced enough that it had been circulated to senior officials, including Speaker of the House Dennis Hastert and Vice President Richard Cheney. Id. Section 126 of that draft legislation is entitled "Equal Access to Consumer Credit Reports," and the draft's legislative history tried to explain that the government was seeking "equal access" to credit reports as is available to private-sector lenders. See Memorandum on

Proposed Domestic Security Enhancement Act of 2003: Section-by-Section Analysis 9 (Jan. 9, 2003), http://www.publicintegrity.org/dtaweb/downloads/Story 01 020703 Doc 1.pdf. In testimony before the House Financial Services Committee, I explained a number of respects in which the government would have greater access, with fewer safeguards, than exists for the private sector. See The Importance of the National Credit Reporting System to Consumers and the U.S. Economy: Hearing Before the Subcomm. on Fin. Inst. and Consumer Credit, the House Comm. on Fin. Servs., 108th Cong. 7-8 (2003), available at www.peterswire.net/2003 05 01 blogarchives.html. This example shows both an example of a ratcheting-up argument and the need to subject such claims for "equal access" to informed scrutiny.

n279. For discussion of the timetable of consideration of the Patriot Act, see Peter P. Swire & Lauren B. Steinfeld, Security and Privacy After September 11: The Health Care Example, 86 Minn. L. Rev. 1515, 1516-17 (2002).

n280. I personally saw many of the electronic surveillance provisions in the course of my work from 1999 until early 2001 while at the Office of Management and Budget.

n281. See supra notes 150, 166 and accompanying text.

n282. Peter P. Swire, Efficient Confidentiality for Privacy, Security, and Confidential Business Information, in Brookings-Wharton Papers on Financial Services 294 (Robert E. Litan & Richard Herring eds., 2003).

n283. Id.

n284. Id.

n285. Christy Harvey, American Opinion (A Special Report): Optimism Outduels Pessimism, Wall St. J., Sept. 16, 1999, at A10.

n286. See infra notes 341-43 and accompanying text (explaining how events at the Abu Ghraib prison illustrate the long-term risks of failing to implement the rule of law).

n287. See supra notes 21-26, 227-42 and accompanying text.

n288. See supra notes 131-34 and accompanying text.

n289. See supra notes 210-11 and accompanying text.

n290. See Electronic Privacy Information Center, supra note 118.

n291. See supra notes 212-21 and accompanying text.

n292. See supra notes 192-99 and accompanying text.

n293. See Electronic Privacy Information Center, supra note 118. Attorney General Ashcroft, in commenting on the FISCR decision, said, "the Court of Review's action revolutionizes our ability to investigate terrorists and prosecute terrorist acts." Attorney General John Ashcroft, Remarks Regarding the Decision of Foreign Intelligence Surveillance Court of Review (Nov. 18, 2002), http://www.usdoj.gov/ag/speeches/2002/111802fisanewsconference.htm. The Attorney General said the FBI "will double the number of attorneys working in its National Security Law Unit to handle FISA applications" and he directed "each U.S. attorney's office [to] designate at least one prosecutor to be a point of contact for purposes of" FISA. Id.

n294. See supra notes 187-88 and accompanying text.

n295. 50 U.S.C. 1807 (2000).

n296. Id. 1808(a)(2).

n297. In full, the annual reports for pen register and trap and trace orders provide:

(1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order; (2) the offense specified in the order or application, or extension of an order; (3) the number of investigations involved; (4) the number and nature of the facilities affected; and (5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

18 U.S.C. 3126 (2000).

n298. 18 U.S.C. 2519(1) (2000).

n299. Id. 2519(2)(b).

n300. Id. 2519(2)(c)-(g).

n301. The annual reports are available at Administrative Office of the United States Courts, Wiretap Reports, http://www.uscourts.gov/wiretap.html (last visited July 29, 2004).

n302. The definition of "agent of a foreign power" is given at 50 U.S.C. 1801 (2000). See supra notes 90-91, 95-96 and accompanying text (discussing "agent of a foreign power").

n303. See CarrieLyn Donigan Guymon, International Legal Mechanisms for Combating Transnational Organized Crime: The Need for a Multilateral Convention, 18 Berkeley J. Int'l L. 53, 59 (2000).

n304. S. Rep. No. 90-1097 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2153-2163. "The major purpose of Title III is to combat organized crime." Id., 1968 U.S.C.C.A.N. at 2153.

n305. Admin. Office of the United States Courts, 2002 Wiretap Report, at tbl. III (2003), http://www.uscourts.gov/wiretap02/contents.html [hereinafter 2002 Wiretap Report]. The comparable figures for 1998 were 458 (81%) narcotics and 58 (10%) racketeering cases out of 566 orders. Admin. Office of the United States Courts, 1998 Wiretap Report, at tbl. III (1999), http://www.uscourts.gov/wiretap98/contents.html.

n306. See supra note 9.

n307. 2002 Wiretap Report, supra note 305, at tbl. III; Electronic Privacy Information Center, supra note 118.

n308. See supra notes 177-86 and accompanying text.

n309. See infra note 324 and accompanying text.

n310. See supra notes 165-76 and accompanying text.

n311. See 50 U.S.C.A. 501 (West 2003).

n312. See generally Kathryn Martin, Note, The USA Patriot Act's Application to Library Patron Records, 29 J. Legis. 283 (2003). Attorney General Ashcroft criticized the American Library Association and others for "baseless hysteria" about the government's ability to pry into the public's reading habits. Eric Lichtblau, Ashcroft Mocks Librarians and Others Who Oppose Part of Counterterrorism Law, N.Y. Times, Sept. 16, 2003, at A23.

n313. Martin, supra note 312, at 291.

n314. See Swire & Steinfeld, supra note 279, at 1516-17 (discussing national security and law enforcement aspects of the federal medical privacy regulation in the wake of the Patriot Act).

n315. See Right to Financial Privacy Act of 1978, 12 U.S.C. 3401-3420, 3422 (2000) (definitions).

n316. For one collection of U.S. privacy statutes, including the provisions for government access to records, see Peter Swire, Privacy Law & Policy Home Page, http://www.peterswire.net/pspriv.html (last visited July 29, 2004).

n317. 45 C.F.R. 164.512(k) (2002).

n318. 12 U.S.C. 3409.

n319. A memorandum from Attorney General Ashcroft to FBI Director Mueller on the subject was released to the press on September 18, 2003. Memorandum from Attorney General to Director Robert S. Mueller (Sept. 18, 2003), available at http://www.cdt.org/security/usapatriot/030918doj.shtml.

n320. See supra notes 177-86 and accompanying text.

n321. See id.

n322. For instance, Senators Leahy, Grassley, and Spector have sponsored S. 436 in the 108th Congress to require such reporting. See S. 436, 108th Cong. (2003).

n323. For example, there could be a minimization procedure where one team could look at the raw data and perform minimization while another team could keep the data for ongoing analysis. The FISC itself might also act as a rulemaker for the orders that come before it, specifying minimization rules just as federal courts play a role in drafting the rules of criminal and civil procedure and the rules of evidence.

A better solution may be to use new technologies that can use cryptographic tools to protect privacy while allowing limited sharing of information upon a proper showing of need. For a joint report on this topic by the Center for Democracy and Technology and the Heritage Foundation, see James X. Dempsey & Paul Rosenzweig, Technologies That Can Protect Privacy as Information Is Shared to Combat Terrorism (May 26, 2004), http://www.cdt.org/security/usapatriot/20040526technologies.pdf.

n324. 50 U.S.C.A. 1861(d) (West 2003).

n325. 18 U.S.C. 2511(2)(a)(ii) (2000).

n326. Katz v. United States, 389 U.S. 347, 355 n.16 (1967) (internal citations omitted).

n327. See Homeland Security Act of 2002, Pub. L. No. 107-296, 212(5), 116 Stat. 2135; see also Gina Marie Stevens, Cong. Research Serv., Homeland Security Act of 2002: Critical Infrastructure Information Act 12-13 (2003), http://www.fas.org/sgp/crs/RL31762.pdf (explaining the intersection of the Homeland Security Act's prohibition on disclosures by federal employees and the Whistleblower Protection Act).

n328. In crafting changes to the scope of the "gag rule," attention should be paid to the broad definition of "material support or resources" used in 18 U.S.C. 2339A and 2339B. Parts of this statute were struck down as unconstitutionally void for vagueness in Humanitarian Law Project v. Ashcroft, 309 F. Supp. 2d 1185, 1198-1201 (C.D. Cal. 2004). The general prohibition against material assistance to terrorism, however, is analogous to the crime of obstruction of justice in the sense that impeding the terrorist investigation can give rise to criminal prosecution. Further study is likely needed to determine the extent to which the material assistance crime would adequately address the concerns of those who are inclined to support the "gag rules."

n329. These additional suggestions are offered as modest safeguards if the "gag rule" is maintained, rather than as affirmatively desirable proposals.

n330. Hearing of the Senate Judiciary Comm.: War Against Terrorism, 108th Cong. 92 (2003) (statement of Attorney Gen. John Ashcroft, advocating that "the wall" no longer exists).

n331. See supra note 77.

n332. See supra notes 153-55.

n333. In re Sealed Case (FISCR Decision), 310 F.3d 717, 735 (Foreign Intel. Surv. Ct. Rev. 2002); see also supra notes 212-33 and accompanying text (critiquing FISCR decision). The FISCR also said that the government need show "a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes." FISCR Decision, 310 F.3d at 735. These easy showings of "significant purpose" would seem to ignore the decision by Congress to raise the Bush administration's proposed language of "a purpose" up to what would have seemed to be the stricter test of a "significant purpose." See supra notes 160-64 and accompanying text.

n334. 50 U.S.C. 1801 (2000).

n335. See supra notes 302-06 and accompanying text.

n336. 18 U.S.C. 2518(3)(C) (2000); see supra notes 100-24 and accompanying text (comparing Title III and FISA legal requirements).

n337. 50 U.S.C. 1804(7)(C).

n338. See In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611, 620 (Foreign Intel. Surv. Ct. 2002).

n339. The methods for creating rules are set forth in the Rules Enabling Act, 28 U.S.C. 2071-2077 (2000). For information on the drafting of the federal rules of procedure and evidence, see the collection of materials maintained at Administrative Office of the United States Courts, Federal Rulemaking, http://www.uscourts.gov/rules/index.html (last revised June 18, 2004).

n340. See 50 U.S.C. 435 (2000).

n341. R. Jeffrey Smith, Memo Gave Intelligence Bigger Role, Increased Pressure Sought on Prisoners, Wash. Post, May 21, 2004, at A17 (quoting memorandum from Lt. General Ricardo S. Sanchez).

n342. E.g., Seymour M. Hersh, Torture at Abu Ghraib, New Yorker, May 10, 2004, at 42, available at http://www.newyorker.com/fact/content/?040510fa fact (discussing report by Major General Antonio M. Taguba and other sources that stressed how military police were supposed to "set the conditions" for military intelligence interrogations).

n343. See supra notes 57-84 and accompanying text for a discussion during the period of "The Lawless State" of the lack of clear rules, the claims to inherent executive discretion to set national security wiretaps, and the centrality of preventing harm, especially by "subversives." Since September 11, the amendments to the Patriot Act, discussed supra at notes 157-90 and accompanying text, have a unifying theme of granting greater discretion to the executive branch, with less judicial oversight. The return in the FBI to a strategy of prevention has been clearly stated by FBI Director Mueller, who has made clear "in essence, we need a different approach that puts prevention above all else." Robert S. Mueller, III, Statement on Press Availability on the FBI's Reorganization (May 29, 2002), http://www.fbi.gov/pressrel/speeches/speech052902. htm.

For the events at Abu Ghraib, the reports available to date indicate: a lack of clear rules about the relative roles of military intelligence and military policy; executive discretion as indicated by reports that senior officials did not support application of Geneva Conventions to prisoners held at Abu Ghraib; and a philosophy that extraordinary measures were justified to gain intelligence information from the persons held there. See generally Hersh, supra note 342.